AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

S. Hrg. 113–425

# THE NAVY YARD TRAGEDY

# HEARING

BEFORE THE

## COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS UNITED STATES SENATE

ONE HUNDRED THIRTEENTH CONGRESS

FIRST SESSION

**EXAMINING GOVERNMENT CLEARANCES AND BACKGROUND CHECKS, OCTOBER 31, 2013**

**EXAMINING PHYSICAL SECURITY FOR FEDERAL FACILITIES, DECEMBER 17, 2013**

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

Printed for the use of the
Committee on Homeland Security and Governmental Affairs

# THE NAVY YARD TRAGEDY

S. Hrg. 113–425

# THE NAVY YARD TRAGEDY

# HEARING

BEFORE THE

## COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS UNITED STATES SENATE

ONE HUNDRED THIRTEENTH CONGRESS

FIRST SESSION

**EXAMINING GOVERNMENT CLEARANCES AND BACKGROUND CHECKS, OCTOBER 31, 2013**

**EXAMINING PHYSICAL SECURITY FOR FEDERAL FACILITIES, DECEMBER 17, 2013**

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

Printed for the use of the
Committee on Homeland Security and Governmental Affairs

U.S. GOVERNMENT PRINTING OFFICE

85–500 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) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

THOMAS R. CARPER, Delaware *Chairman*

CARL LEVIN, Michigan
MARK L. PRYOR, Arkansas
MARY L. LANDRIEU, Louisiana
CLAIRE MCCASKILL, Missouri
JON TESTER, Montana
MARK BEGICH, Alaska
TAMMY BALDWIN, Wisconsin
HEIDI HEITKAMP, North Dakota

TOM COBURN, Oklahoma
JOHN MCCAIN, Arizona
RON JOHNSON, Wisconsin
ROB PORTMAN, Ohio
RAND PAUL, Kentucky
MICHAEL B. ENZI, Wyoming
KELLY AYOTTE, New Hampshire

RICHARD J. KESSLER, *Staff Director*
JOHN P. KILVINGTON, *Deputy Staff Director*
TROY H. CRIBB, *Chief Counsel for Governmental Affairs*
LAWRENCE B. NOVEY, *Chief Counsel for Governmental Affairs*
JASON M. YANUSSI, *Senior Professional Staff Member*
NICOLE B. MAINOR, *U.S. Secret Service Detailee*
KEITH B. ASHDOWN, *Minority Staff Director*
MARK K. HARRIS, *Minority U.S. Coast Guard Detailee*
JAMES P. GELFAND, *Minority Counsel*
CORY P. WILSON, *Minority U.S. Secret Service Detailee*
LAURA W. KILBRIDE, *Chief Clerk*
LAUREN M. CORCORAN, *Hearing Clerk*

# CONTENTS


| | Page |
|---|---|
| Opening statements: | |
| Senator Carper | 1, 141 |
| Senator Coburn | 4, 145 |
| Senator Tester | 4 |
| Senator Ayotte | 26 |
| Senator Heitkamp | 30 |
| Senator McCaskill | 32 |
| Senator Portman | 35 |
| Prepared statements: | |
| Senator Carper | 45, 185 |
| Senator Coburn | 189 |


## WITNESSES

### THURSDAY, OCTOBER 31, 2013


| | |
|---|---|
| Hon. Joseph G. Jordan, Administrator for Federal Procurement Policy, Office of Management and Budget | 7 |
| Hon. Elaine D. Kaplan, Acting Director, Office of Personnel Management | 9 |
| Brian A. Prioletti, Assistant Director, Special Security Directorate, National Counterintelligence Executive, Office of the Director of National Intelligence | 11 |
| Stephen F. Lewis, Deputy Director for Personnel, Industrial and Physical Security Policy, Directorate of Security Policy & Oversight, Office of Under Secretary of Defense for Intelligence, U.S. Department of Defense | 13 |
| Brenda S. Farrell, Director, Defense Capabilities and Management, U.S. Government Accountability Office | 15 |


### ALPHABETICAL LIST OF WITNESSES


| | |
|---|---|
| Farrell Brenda S.: | |
| Testimony | 15 |
| Prepared statement | 72 |
| Jordan, Hon. Joseph G.: | |
| Testimony | 7 |
| Prepared statement | 48 |
| Kaplan, Hon. Elaine D.: | |
| Testimony | 9 |
| Prepared statement | 55 |
| Lewis, Stephen F.: | |
| Testimony | 13 |
| Prepared statement | 68 |
| Prioletti, Brian A.: | |
| Testimony | 11 |
| Prepared statement | 61 |


## APPENDIX


| | |
|---|---|
| Statement from the Professional Services Council | 95 |
| Letter from Ms. Kaplan to Senator Coburn | 101 |
| OPM Whitepaper | 102 |
| Responses for post-hearing questions for the Record from: | |
| Mr. Jordan | 112 |
| Ms. Kaplan | 116 |
| Mr. Prioletti | 123 |
| Mr. Lewis | 129 |

Page

Responses for post-hearing questions for the Record from—Continued
Ms. Farrell ..... 134

TUESDAY, DECEMBER 17, 2013

Caitlin A. Durkovich, Assistant Secretary for Infrastructure Protection, National Protection and Programs Directorate, U.S. Department of Homeland Security ..... 146
Leonard Eric Patterson, Director, Federal Protective Service, National Protection and Programs Directorate, U.S. Department of Homeland Security ..... 148
Stephen F. Lewis, Deputy Director for Personnel, Industrial and Physical Security Policy, Directorate of Security Policy and Oversight, Office of Under Secretary of Defense for Intelligence, U.S. Department of Defense ..... 150
Mark L. Goldstein, Director, Physical Infrastructure Issues, U.S. Government Accountability Office ..... 172
Stephen D. Amitay, Executive Director, National Association of Security Companies ..... 173
David L. Wright, President, Federal Protective Service Union, American Federation of Government Employees ..... 175

ALPHABETICAL LIST OF WITNESSES

Amitay, Stephen D.:
Testimony ..... 173
Prepared statement ..... 221
Durkovich, Caitlin A.:
Testimony ..... 146
Prepared statement ..... 192
Goldstein, Mark L.:
Testimony ..... 172
Prepared statement ..... 210
Lewis, Stephen F.:
Testimony ..... 150
Prepared statement ..... 205
Patterson, Leonard Eric:
Testimony ..... 148
Prepared statement ..... 198
Wright, David L.:
Testimony ..... 175
Prepared statement ..... 239

APPENDIX

DHS Active Shooter updated submitted by Senator Coburn ..... 254
Responses for post-hearing questions for the Record from:
Ms. Durkovich and Mr. Patterson ..... 256
Mr. Lewis ..... 316
Mr. Goldstein ..... 326
Mr. Amitay ..... 330
Mr. Wright ..... 335

# THE NAVY YARD TRAGEDY: EXAMINING GOVERNMENT CLEARANCES AND BACKGROUND CHECKS

---

**THURSDAY, OCTOBER 31, 2013**

U.S. SENATE,
COMMITTEE ON HOMELAND SECURITY
AND GOVERNMENTAL AFFAIRS,
*Washington, DC.*

The Committee met, pursuant to notice, at 10:01 a.m., in room SD–342, Dirksen Senate Office Building, Hon. Thomas R. Carper, Chairman of the Committee, presiding.

Present: Senators Carper, Landrieu, McCaskill, Tester, Heitkamp, Coburn, Portman, and Ayotte.

## OPENING STATEMENT OF CHAIRMAN CARPER

Chairman CARPER. Well, good morning, everyone. The hearing will come to order. Welcome, one and all.

On Monday, September 16, a horrible tragedy unfolded at the Navy Yard in Washington D.C. A very troubled individual took 12 lives in a senseless act of violence. The circumstances that led to this tragedy are multidimensional.

Many of the issues raised by this tragedy—such as the adequacy of our gun laws and the quality of mental health care—are outside the purview of this Committee. But as we have learned more about Aaron Alexis, a number of my colleagues and I have been asking each other why such a troubled, unstable individual possessed a security clearance from the U.S. Government.

Why was he originally granted a security clearance when he did not disclose his arrest record on his application? Why did the investigator responsible for looking into that arrest write up that Alexis had "retaliated by deflating" someone's tires instead of disclosing that Alexis had shot those tires? And we also wonder how such violence could have taken place at the Navy Yard, which is more secure than just about any workplace in our country.

The Navy Yard tragedy is not the only reason that Members of Congress are questioning the quality of the background checks. The Edward Snowden case, of course, raises many of the same questions. So have the Wikileaks disclosures by Private Bradley Manning.

Just yesterday, we learned that the Department of Justice (DOJ) has joined a lawsuit against a company called United States Investigations Services (USIS). This is the company that performs about

45 percent of the background investigations that are contracted out by the Office of Personnel Management (OPM).

According to this lawsuit, USIS engaged in a practice that company insiders referred to as "dumping." Some refer to it as "flushing." Under this alleged scam, USIS would send investigations back to the Office of Personnel Management even though they had not gone through the full review process. Through this dumping, USIS maximized its profits.

Many national security experts have long argued that the security clearance process is antiquated and in need of modernization, and given recent events, I think we have to ask whether the system is fundamentally flawed. But we should also be mindful that, for many years, both Congress and Federal agencies were concerned about the backlog of security clearance applications, which grew larger after September 11, 2001. We need to make sure that investigators do not feel pressured to sacrifice quality for speed.

Many have heard me say that almost everything I do, I know I can do better. The same is true, I think, for all of us and most Federal programs. It is in that spirit Dr. Coburn and I have convened today's hearing. Our primary purpose is to learn what we are doing right in the security clearance process, do more of that, while also learning how we can improve it.

We have many questions to ask, and here are some of them:

Are we looking at the right risk factors in attempting to identify people who should not be trusted with a clearance, or who could do serious harm to our government and our country?

What important information do background checks miss in the current system, which relies heavily on self-reporting by the individuals applying for a clearance?

Once a clearance is granted, what events should trigger a reexamination of an individual's suitability to retain that clearance?

What problems are created by the heavy reliance by the Office of Personnel Management on contractors to perform the background checks?

What are the advantages of that reliance?

And what is the relationship between background checks for security clearances and background checks for other types of privileges, such as access to governmental facilities?

We also need to ask what impacts sequestration and years of strained budgets have had on the clearance process. Under the current system, periodic reinvestigations of individuals holding clearances are supposed to be done every 5 years for people with Top Secret clearances, and every 10 years for people with Secret clearances.

However, because of funding shortfalls, employees sometimes continue to work in positions that allow access to classified information, even if the initial period of clearance has lapsed. For example, this summer, for 10 weeks the Department of Defense (DOD) suspended the periodic reviews of some contractor employees due to funding shortfalls.

I would like to hear from our witnesses today about how often suspensions like that are happening across the Federal Government. I would also like to hear about what agencies are doing to

manage risks to our security when clearances are not reexamined on schedule through the periodic review process.

Today, we have been joined by officials from the four agencies responsible for the policies and procedures used to determine who is eligible to obtain security clearances and access to government facilities and computers. They are the Office of Management and Budget (OMB), the Office of Personnel Management, the Office of the Director of National Intelligence (ODNI), and the Department of Defense.

We want these officials to talk with us this morning about the critical security related policies and procedures and also about the coordinated reviews of these processes now underway throughout the government in the aftermath of the Navy Yard tragedy and other recent incidents. We also will hear from an expert at the Government Accountability Office (GAO), which has produced a wide body of work on the security clearance process. Welcome.

This hearing builds on the ongoing good work of our Subcommittees, which held a hearing on security clearances just this past June under the able leadership of Senators Tester, Portman, McCaskill, and Johnson. That hearing exposed the urgent need for additional resources for the Inspector General (IG) at the Office of Personnel Management to enable that IG to conduct important oversight of background investigations.

In July, our Committee approved a portion of a bill sponsored by Senator Tester and cosponsored by Dr. Coburn, Senator McCaskill, Senator Portman, Senator Begich, Senator Johnson, Senator Nelson, and Senator Baucus to allow the Inspector General to tap into OPM's revolving fund for the purposes of performing that much needed oversight, and we commend Senator Tester and our colleagues, for their good work. The legislation passed the Senate earlier this month, and my hope is it will be signed into law by the President soon.

In closing, I want to say that the vast majority of individuals who hold security clearances are honorable and trustworthy people. Many of them felt called into service after September 11, 2001, to help protect our country, and they deserve our thanks. Having said that, though, we still must have a system that does a better job of rooting out those with nefarious purposes and those who become deeply troubled and unstable. That system must identify those whose behavior signals an unacceptable risk to be entrusted with classified information or access to sensitive Federal facilities. I hope that our hearing today will help point us to a number of sensible solutions that—taken together—will truly improve our national security.

Finally, I think it is important to note that our Committee continues to look at other aspects of the Navy Yard tragedy, including the physical security of Federal buildings, as well as preparedness, emergency response, and communications issues. So, we have much work to do to learn as much as we can from this tragedy and try to prevent similar ones from occurring in the future.

With that, let me welcome Dr. Coburn and say that I look forward to his opening comments, and then we will turn to our witnesses. Dr. Coburn, welcome.

## OPENING STATEMENT OF SENATOR COBURN

Senator COBURN. Well, thank you, Chairman Carper, and welcome to our witnesses.

First, let me extend my deepest condolences to the families, coworkers, and friends of those that were lost on September 16. To me this is not a political issue. This is an issue of us failing to do our job in a proper way when it comes to security clearances.

Today GAO is releasing a report that shows some 8,400 people received security clearances while they had tax debts, which is a vulnerability. And the vast majority of those were Top Secret security clearances. So our process is obviously broken, not complete, and not adequate.

Until this year, OPM did not even have the means of debarring persons or companies that falsified background checks for clearances. Worse, OPM's IG recommended debarment of 22 individuals, have received no answer on 14 of the cases, and have been informed that the other 8 would not be debarred. Something is very wrong.

It is unlikely that a stricter clearance process would have prevented a deranged individual from committing murder, but this event should be a catalyst for Congress to try to fix the way this country categorizes, handles, and grants access to sensitive data.

Two problems. One, there is way too much stuff that is classified that does not need to be classified. And, two, there are way too many security clearances approved. So if you markedly increase the amount of material that does not need to be classified, you have to increase the number of people that need to have access to it.

So we need to address both problems. I look forward to going through the comments today and with our panel of witnesses and get closer to the real answers, and, Chairman Carper, I thank you again for holding this hearing, and I appreciate the work of Senator Tester.

Chairman CARPER. Thank you, Dr. Coburn.

I am going to ask Senator Tester, before we turn to the witnesses, to make some comments as well and, again, to commend——

## OPENING STATEMENT OF SENATOR TESTER

Senator TESTER. Yes, I would like to. Thank you, Chairman Carper, and I want to thank Dr. Coburn for his leadership on this issue as well.

It was 4 months ago when we had the hearing after the Snowden leaks, Senator Portman and I had. In fact, Stephen Lewis and Brenda Farrell were part of that panel, and I want to thank you for being here today as well as last time.

In my opening remarks, I said that, given the fiscal and security stakes involved, we had to get it right and there was no margin for error. The fact was, as we knew then, as we know today, we need to make immediate reform of the process. There needs to be more transparency. There needs to be more oversight.

The outcome of that hearing was a bill that the Chairman talked about introduced by myself as well as Senators Portman, McCaskill, Johnson, and Coburn. A provision of that legislation, known as the "SCORE Act," subsequently passed the Senate. When

signed into law, it is going to bring better oversight to the background investigations conducted by OPM and its contractors.

But there are two other provisions that are also very important that we need to get across the finish line that dealt with the issues that Senator Coburn talked about with the number of security clearances given and, quite frankly, another issue that deals with what do we do when we have a company that screws up and screws up with some regularity. It is too important. And we saw that with the attacks on September 16 when 12 good men and women left for home, as they did most every other Monday morning. Within a couple of hours, no warning, no motive, they were killed by a man with a history of mental illness, a pattern of violent behavior, and a criminal record—a man who was cleared by our government through a contractor as someone who should have access to this Nation's most secure facilities and sensitive information.

Look, there are real-life consequences for failures within our government, and we need answers, we need solutions, we need action, because, quite frankly, the men and women who rely on that action deserve no less.

I would just say thank you, Mr. Chairman, for having this hearing. It would seem to me that it is critically important that we act as efficiently and as thoughtfully as possible to get this problem solved because it is obviously a problem and a big one.

Chairman CARPER. Thank you, and thanks for your leadership and your good work and that of Senator Portman and others who joined you in it.

Let me now turn to our panel and introduce each of our distinguished witnesses.

The first witness is the Hon. Joseph Jordan, Administrator of the Office of Federal Procurement Policy at the Office of Management and Budget. Who do you report to?

Mr. JORDAN. I report to Beth Cobert, the newly confirmed Deputy Director.

Chairman CARPER. We have heard of her.

Mr. JORDAN. Thank you for your——

Chairman CARPER. We got her through very quickly. I want to thank Dr. Coburn and others, Senator Johnson and others, and actually John Cornyn was very helpful in trying to expedite that, and we are delighted that we got her through almost in record time.

Mr. JORDAN. We sincerely appreciate it.

Chairman CARPER. I think Sylvia Burwell has a top-flight leadership team there. We expect a balanced budget in about 2 years.

Our first witness is Joe Jordan from OMB. Welcome. Mr. Jordan was confirmed as the Administrator for Federal Procurement Policy (FPP) in May 2012. He is responsible for developing and implementing government contracting policies and as the senior leader and formal adviser to the OMB Director, he will speak to OMB's role in the security clearance process. Again, we thank you for your testimony and for your service.

Our next witness is Elaine Kaplan, the Acting Director of the Office of Personnel Management, a position she has held since April 2013. I understand she has been confirmed for a new job. Is that true? Do you want to tell us what it is?

Ms. KAPLAN. Yes. I have been confirmed to be a judge on the United States Court of Federal Claims.

Chairman CARPER. Did any of us vote for you?

Ms. KAPLAN. Some of you did. The others were clearly mistaken. [Laughter.]

Chairman CARPER. Congratulations, and thank you for doing double duty here in the last 6 months and taking this on. And to our colleagues who were good enough to find their way to supporting a confirmed Director, Ms. Archuleta, thank you for your support.

As the Acting Director, Ms. Kaplan oversees the Office of Federal Investigative Services (FIS). This office is responsible for ensuring that the Federal Government has a workforce that is worthy of the public trust by investigating and reviewing applications for security clearances and by performing background checks to determine whether a person is suitable for employment by the Federal Government or Federal contractor.

Acting Director Kaplan, thank you for your testimony, for your leadership all these months, and good luck in what lies ahead.

Our next witness is Brian Prioletti, an Assistant Director in the Special Security Directorate at the Office of the Director of National Intelligence. Mr. Prioletti has served in this position since May 2013 after serving at the Central Intelligence Agency (CIA) from 1981 to 2013. As the Assistant Director of the Special Security Directorate, Mr. Prioletti is responsible for leading the oversight and reform efforts of the security clearance process on behalf of the Director of National Intelligence (DNI).

We thank you for that, and we thank you for all your service to our country and for joining us today.

Our next witness is Stephen Lewis, the Deputy Director for Personnel, Industrial and Physical Security Policy in the Office of the Under Secretary for Intelligence at the Department of Defense. The Under Secretary of Defense for Intelligence (USDI) is responsible for DOD's policies, programs, and guidance related to, among other things, personnel and facility security.

Mr. Lewis, we thank you for your testimony today, and we are delighted to note—I mentioned to Dr. Coburn that in the audience today is your daughter, Sara, who for a number of years was my scheduler. She told me where to go every day, with relish, and I usually went there—not always on time. But we welcome both you and Sara.

The Under Secretary for Defense Intelligence is responsible for DOD policies, programs, and guidance related to, among other things, personnel and facility security. You have that whole broad realm?

Mr. LEWIS. Yes, we do.

Chairman CARPER. All right. And how long have you been doing this?

Mr. LEWIS. Six years now.

Chairman CARPER. All right. Thank you.

Our final witness is Brenda Farrell, the Director of Defense Capabilities and Management at the Government Accountability Office. In April 2007, Ms. Farrell was appointed to serve as Director in GAO's Defense Capabilities and Management team where she is

responsible for military and civilian personnel issues, including personnel security clearance process issues. Ms. Farrell has authored several GAO reports critiquing governmental efforts to reform the security clearance process. We thank you for your testimony today and earlier before Senator Tester's Committee.

Before turning it over to Mr. Jordan for his remarks, we had a short scrum before the hearing began in the anteroom. Ms. Farrell was not, I do not think, present in the anteroom, but what I said to our witnesses, colleagues, and guests, I said part of what we are trying to do here is figure out what is the role of government. I quoted Abraham Lincoln, who used to say, "The role of government is to do for the people what they cannot do for themselves." And David Osborne more recently said in a book called "Reinventing Government," that the role of government is to steer the boat, not to row the boat. And here today we hopefully are going to figure out better what is the role of government, what kind of steering do we need to do, and who should be doing the rowing, and how do we make sure that we are steering better; but whoever is doing the rowing, whether it is the public sector, the Federal Government, or the private sector, they are doing a much better job than they have done here of late.

Mr. Jordan, you have roughly 5 minutes to give us your statement. If you go way beyond that, we will rein you in, but stick to that and we will be just fine. Thanks so much.

**TESTIMONY OF THE HON. JOSEPH G. JORDAN,[1] ADMINISTRATOR FOR FEDERAL PROCUREMENT POLICY, OFFICE OF MANAGEMENT AND BUDGET**

Mr. JORDAN. Thank you.

Chairman Carper, Ranking Member Coburn, and Members of the Committee, I appreciate the opportunity to appear before you today to discuss the government's practices and procedures regarding security clearances, facility access, and suitability determinations.

Before I begin my testimony, I wanted to first say a few words about the tragic events that occurred at the Washington Navy Yard on September 16. On behalf of the Administration and my colleagues here today, I want to extend our deepest condolences to all those affected by this tragedy. While nothing can bring back the loved ones who died that day, it is clear that collectively we need to do a better job of securing our military facilities and deciding who gets access to them.

I and my fellow witnesses take this responsibility incredibly seriously and are deeply and personally committed to this effort.

I also wanted to note that, to assist with addressing the full spectrum——

Chairman CARPER. Mr. Jordan, sorry to interrupt. I said 5 minutes. You have seven. I think you were told you have 7 minutes, so take seven.

Mr. JORDAN. OK. Thank you, Mr. Chairman.

Chairman CARPER. You can take less. [Laughter.]

Try not to take any more.

[1] The prepared statement of Mr. Jordan appears in the Appendix on page 48.

Mr. JORDAN. I shall. I also wanted to note that, to assist with addressing the full spectrum of needs of all individuals affected by the tragedy, we have established the Washington Navy Yard Recovery Task Force, led by the Assistant Secretary of the Navy for Energy, Installations, and the Environment.

As government officials, our highest duty is to protect the national security, including the confidentiality of classified information. Simultaneously, we have a critically important obligation to protect individuals performing work on behalf of Federal agencies from workplace violence. In recent years, with Congress' help, we have taken a number of important actions to strengthen protections of both national security information and the physical security of Federal facilities, such as improving the effectiveness and efficiency of background investigations and strengthening the processes by which agencies make national security and suitability determinations. We must ensure those processes for granting or revoking access to facilities and information systems fully mitigate risks.

We have a multisector workforce, comprised of military, civilian, and contractor personnel. We have worked to ensure that robust vetting policies and processes are applied to all individuals with access to Federal facilities, networks, or classified information in a consistent manner. This approach reflects two important principles: First, the need to protect our national security is no less critical when the work is performed by contractors than when it is performed by Federal employees; second, the men and women who make up the contractor workforce are no less patriotic than their government counterparts, and in fact, many have had meaningful careers as Federal employees or in the Armed Forces.

While we have made significant progress in the area of fitness and suitability, security clearance, and credentialing process reform, we need to do more.

In 2004, Congress passed the Intelligence Reform and Terrorism Prevention Act (IRTPA), which required all agencies to complete 90 percent of their security clearances in an average of 60 days.

As a result of actions the executive branch has taken to meet the goals and objectives of that act, by December 2009 compliance was achieved. We have consistently met these goals every quarter since, while maintaining the standards expected of the clearance process, and the backlog of initial investigations has been eliminated.

Importantly, executive branch reform efforts have also extended beyond just meeting timeliness goals. In order to align suitability and national security policies and practices and to establish enterprise information technology standards to improve efficiency and reciprocity, we established the Suitability and Security Clearance Performance Accountability Council (PAC). It is chaired by OMB's Deputy Director for Management and accountable to the President for reform goals.

As a marker of the significant progress made, in 2011 GAO removed DOD's Personnel Security Clearance Program from its high-risk list. However, we recognize the serious nature of recent events and will continue to intensify our efforts to strengthen and improve our existing policies and processes. To that end, the President directed OMB to lead a 120-day interagency review of suitability and

security processes. For suitability and fitness, the review will focus on whether the processes in place adequately identify applicants who, based upon their character and past conduct, may be disruptive to operations or even dangerous to the workplace. The focus on national security risk will center on determining eligibility and granting access that could lead to loss of classified information and damage to national security. Additionally, we will evaluate the means to collect, share, process, and store information that supports these decisions, while emphasizing transactions among and equities shared across agencies.

As part of these efforts, we will also be considering opportunities to improve the application of these standards and procedures to contracting, which may include, as just one example, improved information sharing between agencies suspending and debarring officials and the offices responsible for making determinations for fitness and security clearances.

Our first interagency meeting is scheduled for next week and will serve to launch our review process. Additional meetings will occur over the coming weeks, and we fully anticipate this review to be completed within the 120-day timeframe.

Once again, thank you for the opportunity to testify. As I noted in the beginning of my testimony, there is nothing more important than the two goals of protecting our people and protecting our sensitive information. We have steadfastly worked in a collaborative manner to improve our processes and procedures to ensure the safety of both. As recent tragic events have highlighted, however, we must maintain a strong focus on continuous improvements, and we will heed the President's call to conduct a comprehensive review and address any potential gaps in the most effective and quickest manner possible. We look forward to working with this Committee and Congress as we undertake this important work.

Chairman CARPER. Mr. Jordan, thank you so much.

Ms. Kaplan, please.

## TESTIMONY OF THE HON. ELAINE D. KAPLAN,[1] ACTING DIRECTOR, OFFICE OF PERSONNEL MANAGEMENT

Mr. KAPLAN. Chairman Carper, Ranking Member Coburn, and Members of the Committee, thank you for asking me to be here today. The events that occurred last month at the Navy Yard were horrifying and heartbreaking. Twelve civilian employees, among them both civil servants and members of our contract workforce, were ruthlessly gunned down. All of these individuals were doing what millions of their colleagues in the Federal workforce across the country do every day: coming to work to serve the American people, put food on their tables, and provide for their families.

As the Acting Director of the Office of Personnel Management and the Federal Government's Chief Personnel Officer, I share your commitment and that of our President to identifying and addressing the root causes of this terrible tragedy. I also share your commitment and that of my colleagues seated at this table to perfecting, to the greatest extent humanly possible, our processes and procedures for determining who shall be allowed access to our Na-

[1] The prepared statement of Ms. Kaplan appears in the Appendix on page 55.

tion's secrets, granted the privilege of serving in a position of public trust, or given permission to enter Federal buildings and facilities like the Navy Yard.

To those ends, since 2008 OPM, OMB, DOD, and ODNI have worked diligently together on a reform effort to ensure that there is an efficient, aligned, high-quality, and cost-effective system for conducting background investigations and making determinations regarding security clearances, employee suitability, and contractor fitness. We have made great progress, as is reflected in the written testimony of the witnesses at this table. So as Mr. Jordan just mentioned, we have eliminated the backlog of security clearance investigations that in and of themselves posed a risk to our national security. We have dramatically reduced the time it takes to complete such investigations to meet the deadlines that Congress has established. We have imposed reciprocity requirements for greater efficiency, issued new investigative standards that we are now preparing to implement. We have enhanced and professionalized the training of investigators and adjudicators, and we have worked together to implement GAO's very helpful recommendations by designing and imminently deploying a new set of agreed upon metrics that we can use to measure and drive up the quality of our investigative products.

At OPM we have implemented our own new quality control measures and have an aggressive program to hold investigators to the highest standards of integrity and to ensure that their work product is something on which Federal agencies should be able to rely with confidence.

We have overhauled and improved our processes for reviewing the work of our investigators, increased our oversight staff, and are retooling our audit process. We do not tolerate fraud or falsification. We actively look for it, and in those few cases where we find it, we take immediate administrative action and then work, as we have, with our IG and the Department of Justice to pursue criminal sanctions against those who betray the trust that has been bestowed upon them.

Of course, much more remains to be done. Even the highest quality and most comprehensive background investigation is just a snapshot in time. The evolution of the security clearance process has to include the ability to obtain and easily share relevant information on a more frequent or real-time basis.

We also need to improve our capacity to receive information in machine-readable form and to share information across the Federal Government and with State and local law enforcement.

At the President's direction and under the leadership of the Director of OMB, OPM has been and will continue to work with its colleagues on the Performance Accountability Council to conduct the 120-day review of the oversight, the nature and implementation of national security, credentialing and fitness standards for individuals working at Federal facilities. Our review will focus on steps that can be taken to strengthen these processes and the implementation of solutions.

The tragic events at the Navy Yard as well as recent high-profile security breaches highlight the need to be ever vigilant in ensuring that individuals entrusted with access to classified information,

and, more generally, individuals with physical access to Federal facilities and information do not present a risk of harm to the national security or to the safety of our employees in our workplaces, and to the end of improving our processes and procedures.

I thank you for the opportunity to testify regarding all of these issues, and I will be happy to answer any questions that you might have. Thank you.

Chairman CARPER. Ms. Kaplan, thank you for that, and for those encouraging words.

Mr. Prioletti, please proceed. Again, thanks for joining us.

**TESTIMONY OF BRIAN A. PRIOLETTI,[1] ASSISTANT DIRECTOR, SPECIAL SECURITY DIRECTORATE, NATIONAL COUNTER-INTELLIGENCE EXECUTIVE, OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE**

Mr. PRIOLETTI. Good morning, Chairman Carper, Ranking Member Coburn, and distinguished Members of the Committee. Thank you for the invitation to provide information on the government's practices and procedures regarding security clearances and background investigations. My statement will address the role of the Director of National Intelligence, as Security Executive Agent, has authority and responsibility for oversight of the security clearance process across the government, areas in need of attention in the current process, and initiatives underway to address those areas. Before I followup, I would like to make the comment that we also add our deepest condolences to the family members for their loss and our commitment to work toward continuing to improve the security processes and access capabilities of the U.S. Government.

Pursuant to Executive Order (EO) 13467, the DNI, as the Security Executive Agent, is responsible for the development and oversight of effective, efficient, uniform policies and procedures governing the timely conduct of investigations and adjudications for eligibility for access to classified information or eligibility to hold a sensitive position. The DNI also serves as the final authority to designate agencies to conduct background investigations and determine eligibility for access to classified information and ensures reciprocal recognition of investigations and adjudication determinations among those agencies.

I would like to focus on two essential components of the security clearance process: The background investigation and adjudicative determination.

The 1997 Federal Investigative Standards (FIS), as amended in 2004, are the current standards used to conduct background checks or investigations. These checks are required prior to making a determination for eligibility for access to classified information or eligibility to occupy a sensitive position.

The scope of the background investigation is dependent upon the level of the security clearance required. Regardless of the type of clearance involved, identified issues must be fully investigated and resolved prior to any adjudication. An adjudicative determination is based upon Adjudicative Guidelines issued by the White House in 2005.

[1] The prepared statement of Mr. Prioletti appears in the Appendix on page 61.

Clearance decisions are made utilizing the whole-person concept, which is a careful weighing of available, reliable information about the person, both past and present, favorable and unfavorable.

Recently, two highly publicized and critical events involving individuals with clearances highlighted areas in need of attention in the current security clearance process. The ODNI, in collaboration with our colleagues here—OMB, OPM, DOD, and other Federal partners—has been leading security clearance reform now for several years. Although these efforts are still a work in progress, when mature, they will mitigate many of these gaps and enhance the Nation's security posture.

Under current policies and practices, an individual's continued eligibility for access to classified information relies heavily on a periodic reinvestigation—essentially a background investigation and adjudication conducted every 5 years for a Top Secret clearance and every 10 years for a Secret clearance. The time interval between periodic reinvestigations leaves the U.S. Government uninformed as to behavior that potentially poses a security or counterintelligence risk.

Continuous Evaluation (CE), is a tool that will assist in closing this information gap. CE allows for ongoing reviews of an individual with access to classified information, or in a sensitive position, to ensure that that individual continues to meet the requirements for eligibility.

CE, as envisioned in the reformed security clearance process, includes automated record checks of commercial databases, government databases, and other lawfully available information. A number of pilot studies have been initiated to assess the feasibility of automated record checks and the utility of publicly available electronic information. More research is required at this time to assess resource impacts and determine the most effective practices.

A robust CE capability will also support and inform the Insider Threat Programs. We must build an enterprise-wide CE program that will promote the sharing of trustworthiness, eligibility, and risk data within and across government agencies to ensure that information is readily available for analysis and action.

Another area in need of attention is consistency and quality of investigations and adjudications. The revised Investigative Standards, when implemented, will provide clear guidance on issue identification and resolution. In addition, the ODNI, OPM, and DOD are co-chairing a working group that is developing common standards and metrics to evaluate background investigations for quality and comprehensiveness. Furthermore, the ODNI has hosted a working group to refine the Adjudicative Guidelines, and recommendations regarding these guidelines are in the policy development phase.

Another initiative supporting a more robust security clearance process was the development of the National Training Standards, which were approved in August 2012 by the DNI and the Director of OPM for implementation in 2014. These standards create uniform training criteria for background investigators, national security adjudicators, and suitability adjudicators.

Additionally, OMB, ODNI, and OPM are working to revise Standard Form 86, the Questionnaire for National Security Posi-

tions, to improve the collection of accurate information pertinent to today's security and counterintelligence concerns.

As a final note, per the President's direction, OMB is conducting a review of the security and suitability processes. As such, the DNI, OPM, and DOD will review the policies, processes, and procedures related to the initiation, investigation, and adjudication of background investigations for personnel security, suitability for employment, and fitness to perform on a contract.

In closing, I want to emphasize the DNI's resolve to lead the initiatives discussed today and continue the collaborative efforts established with OMB, DOD, OPM, and our Federal partners. We thank you for the opportunity to update the Committee at this time and look forward to working with you on these matters.

Chairman CARPER. Mr. Prioletti, thank you for that update.

We now look forward to hearing from Mr. Lewis.

**TESTIMONY OF STEPHEN LEWIS,[1] DEPUTY DIRECTOR FOR PERSONNEL, INDUSTRIAL AND PHYSICAL SECURITY POLICY, DIRECTORATE OF SECURITY POLICY & OVERSIGHT, OFFICE OF UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE, U.S. DEPARTMENT OF DEFENSE**

Mr. LEWIS. Good morning.

Chairman Carper, Ranking Member Coburn, and distinguished Members of the Committee, I appreciate the opportunity to appear before you today to address the practices and procedures in the Department of Defense regarding security clearances, facility access, and background investigations.

The Under Secretary of Defense for Intelligence Dr. Michael Vickers is the Principal Staff Assistant to the Secretary and Deputy Secretary for security matters. In this capacity, Dr. Vickers exercises his authority as the senior official for DOD's personnel security program and has primary responsibility for providing and approving guidance, oversight, and development for policy and procedures governing civilian, military, and industrial base personnel security programs within the DOD.

In order to address the Department's personnel security policies, I believe it is important to first identify the national level policy framework. Executive Order 13467 designates the Director of National Intelligence as the Security Executive Agent with the responsibility to develop uniform policies and procedures to ensure effective completion of investigations and determinations of eligibility, for access to classified information or to hold National Security Positions, and this includes reciprocal acceptance of those determinations. In addition, the Executive Order designates the Director of the Office of Personnel Management as the Suitability Executive Agent, with responsibility for developing and implementing uniform and consistent policies and procedures regarding investigations and adjudications relating to determinations of suitability and eligibility for logical and physical access to Federal Government installations and systems. Finally, the Executive Order creates a Performance Accountability Council, chaired by the Deputy Director for Management at OMB and including the DNI and the

[1] The prepared statement of Mr. Lewis appears in the Appendix on page 68.

Director of OPM, with the responsibility to align suitability, security, and, as appropriate, contractor fitness investigative and adjudicative processes.

With regard to the oversight roles within the DOD, the heads of DOD components are responsible for establishing and overseeing implementation of procedures to ensure prompt reporting of significant derogatory information, unfavorable administrative actions, and adverse actions related to personnel, and this needs to be provided to appropriate officials within their component and, as applicable, to the DOD Consolidated Adjudication Facility. This responsibility applies to military service members, DOD civilians, and contractor personnel.

Under the National Industrial Security Program (NISP), cleared contractors are required to report adverse information coming to their attention regarding their cleared employees. In addition, the Defense Security Service (DSS) is responsible for conducting oversight of companies cleared to perform on classified contracts for DOD and 26 other Federal departments and agencies that use DOD industrial security services.

The Department has worked very hard to create improvements that produced greater efficiencies and effectiveness in the phases of initiating and adjudicating background investigations. As a result, in 2011, the Government Accountability Office removed DOD's personnel security clearance program from the high-risk list.

We have used multiple initiatives to review and confirm the quality of the investigative products we receive, the quality of our adjudications, and the accuracy and the completeness of the documentation of the adjudicative rationale which is the basis for these determinations. This helps to support our oversight as well as reciprocity. In addition, we have implemented a certification process for DOD personnel security adjudicators, and over 90 percent of these adjudicators are certified to rigid standards, and ultimately it is a condition of employment that each adjudicator will complete this certification process.

In May 2012, the Deputy Secretary of Defense directed the consolidation of all adjudicative functions and resources, except for DOD Intelligence Agencies, at Fort Meade, Maryland, under the direction, command, and control of the Director of Administration and Management (DA&M). This decision was made in order to maximize the efficiencies realized by the collocation of the Centralized Adjudications Facilities (CAFs) under the 2005 round of Base Realignment and Closure (BRAC). And effective October 1, the DOD CAF assumed responsibility to adjudicate background investigations which are the basis for the issuance of Common Access Cards (CACs) used for physical access to DOD installations and access to DOD information systems.

Thank you for your time, and I look forward to answering your questions.

Chairman CARPER. Thank you very much.

Brenda Farrell, It is great to see you. Welcome. Please proceed.

**TESTIMONY OF BRENDA S. FARRELL,[1] DIRECTOR, DEFENSE CAPABILITIES AND MANAGEMENT, U.S. GOVERNMENT ACCOUNTABILITY OFFICE**

Ms. FARRELL. Thank you very much. Chairman Carper, Ranking Member Coburn, Members of the Committee, thank you so much for this opportunity to be here today to discuss the Federal Government's personnel security clearance process. Let me briefly summarize my written statement for the record and to some extent what has already been conveyed here today.

Personnel security clearances allow for access to classified information on a need-to-know basis. Recent events, such as the unauthorized disclosure of classified information, have shown that there is much work to be done by Federal agencies, as you noted, Mr. Chairman, to help ensure the process functions effectively and efficiently so that only trustworthy individuals hold security clearances.

Over the years, GAO has conducted a body of work on personnel security clearance issues that gives us a unique historical perspective. My remarks today are based on our reports issued from 2008 through 2013 on DOD's personnel security clearance program and governmentwide reform efforts. My main message today is that quality—and, importantly, quality metrics—needs to be built into every step of the clearance process.

My written statement is divided into two parts.

The first addresses the overall security clearance process. Multiple executive branch agencies are responsible for different steps of the multiphased personnel security clearance process that includes: (1), determination of whether a position requires a clearance; (2), application submission; (3), investigation; (4), adjudication; and, (5), possible appeal if a clearance is denied or revoked.

For example, in 2008, Executive Order 13467 designated the DNI as the Security Executive Agent. As such, the DNI is responsible for developing policies and procedures to help ensure the effective, efficient, and timely completion of background investigations and adjudications relating to determinations of eligibility for access to classified information. In turn, executive branch agencies, such as DOD that accounts for the vast majority of personnel security clearances, determine which of their positions—military, civilian, or contractors—require access to classified information and, therefore, which employees must apply for and undergo a clearance investigation.

Investigators, often contractors for OPM, conduct these investigations for most of the government. OPM provides the resulting investigative report to the requesting agencies for their internal adjudicators to make the decision as to whether or not the person is eligible to hold a clearance. In 2012, we reported that there were issues with the first step of the process: Determining which positions require access to classified information. We reported that the DNI, as Security Executive Agent, had not provided agencies clearly defined policies and procedures to consistently determine if a position requires a clearance or establish guidance to require agencies to review and validate existing Federal civilian positions.

[1] The prepared statement of Ms. Farrell appears in the Appendix on page 72

We recommended that the DNI, in coordination with OPM, issue such guidance, and ODNI concurred with our recommendations. I am pleased to say that the DNI and OPM have actions underway to address our recommendations, and we will continue to monitor their actions.

The second part of my statement addresses the extent to which executive branch agencies have metrics to help determine the quality of the security clearance process. For more than a decade, GAO has emphasized the need to build and monitor quality throughout this personnel security clearance process to promote oversight and positive outcomes, such as maximizing the likelihood that individuals who are security risks will be scrutinized more closely.

For example, GAO reported in 2009 that, with respect to initial Top Secret clearances adjudicated in July 2008 for DOD, documentation was incomplete for most OPM investigations. We independently estimated that 87 percent of 3,500 investigative reports that DOD adjudicators used to make clearance eligibility decisions were missing some required information, such as verification of all of the applicant's employment. We also estimated that about 12 percent of the 3,500 reports did not contain the required subject interview.

In 2009, we recommended that OPM measure the frequency with which its investigative reports met Federal investigative standards in order to improve the quality of investigative documentation. As of August 2013, OPM had not implemented this recommendation.

Finally, I would like to note that we initially placed DOD's clearance program on our high-risk list in 2005 because of delays in processing clearances, and we continued that designation until 2011, when we removed DOD's program in large part due to the significant progress in reducing the amount of time to process a clearance and steps DOD had taken to help ensure the quality of the adjudication process.

At that time we noted executive branch efforts underway to develop and implement metrics to measure the completeness of OPM's investigations provided to DOD. Unfortunately, these efforts have not been realized.

The progress that was made with respect to reducing the amount of time to process clearances would not have been made possible without the committed and sustained oversight by Congress and the executive branch agency leadership. Further actions are needed now to oversee quality at every step of the process, including background investigations.

Mr. Chairman, this concludes my remarks. I would be pleased to take questions when you are ready.

Chairman CARPER. Great. Thanks so much for your testimony. Thanks for your good work in this area, and to all of you for your work in this area.

After I ask some questions, Dr. Coburn will be recognized, then Senator Tester, and then in the following order: Senator Ayotte, Senator Heitkamp, Senator Landrieu, Senator McCaskill, and Senator Portman. Some of those folks have slipped out, but they will come back.

I just want to start with you, Ms. Farrell, if I could. We appreciate very much your formal testimony. I want to just have a less

formal conversation. Of the things that we have heard from each of our witnesses, about the changes that are being made, the reforms that are being adopted or have been adopted, what should we feel especially good about?

Ms. FARRELL. I think the collaboration between DNI and OPM and the other agencies has improved over the years. I think when we started this work back in 2005 looking at timeliness issues, there was not a lot of collaboration and communication going on. I think that Executive Order 13467 that established the Performance Accountability Council and appointed the Deputy Director for Management at OMB as the Chair helped provide a governance structure for that collaboration to continue.

The most notable improvement that we have seen is with the processing of initial personnel security clearances at the top secret level. There are no metrics for the processing times for other aspects, such as the periodic reinvestigations, and, again, our concern has been—and we have stated this over the years since 2005—that we do not want to see the processing of the clearances expedited at the expense of the quality of the investigations.

Chairman CARPER. All right. Of the work that is in progress, some of which we heard discussed today, would you just talk with us for a little bit about what are some of the most important aspects of that work that are in progress, and with a thought of how we in the legislative branch can be helpful, most helpful in expediting that work that is in progress?

Ms. FARRELL. Yes, I think the work that the agencies are doing to revisit the investigative standards is very important. This gets to the heart of what we are saying about quality. By quality, we mean for the background investigations in particular, are we obtaining the right information, the best available information from the right sources? Is it complete? Is it reliable?

So I think revisiting the Federal Investigative Standards and seeing if there are new techniques or new information that needs to be included—and perhaps some needs to be excluded since these standards go back decades. But that is, I think, a very good focus: First determine if you are collecting the information that you need for the background investigations, and then make sure that you have metrics for the completeness of that information.

Chairman CARPER. The second half of my question is advice you might have for this oversight Committee to try to make sure that the work that is in progress, some of the most important work that is in progress, is actually accomplished. Your advice to us?

Ms. FARRELL. Yes. I think part of the reason that we saw progress with the timeliness issue was due to congressional oversight, as I noted in the opening and in my statement. Also at that time, the Intelligence Reform and Terrorism Prevention Act of 2004 required an annual report to Congress for interim steps to meet the final goal of processing clearances within a 60-day period. The good thing was it was not something expected to happen overnight. Again, there were interim steps for the executive branch to take to meet that 60-day goal.

That annual report reflected information on timeliness to help make sure that they were meeting those interim goals, and if they

were not meeting them, what could they do to make a course correction in order to continue that significant progress?

There was a sunset clause on that annual reporting, and we have not had the same type of oversight for the remainder of the reform efforts as we did for timeliness. So I think this may be an area, either through reporting or through continued congressional hearings, with interim steps to help meet the goals.

One of the areas we have concerns is on metrics. In May 2010, several of the executive branch leaders signed a memo to some congressional leaders noting metrics under development that they were planning to put in place, and this covered not only timeliness but the investigations, the adjudications, and reciprocity. A lot of these metrics dealt with quality of the process. But those metrics, as I have noted, with the exception of timeliness, have not been fully developed, and this is something that we would like to understand why not, what is the plan to proceed?

Chairman CARPER. All right. Thank you. I want to drill down a little bit, if I could, on the issue of quality control. Yesterday the Department of Justice announced, I believe, that it is joining a lawsuit brought against the United States Investigations Services, a company that performs about almost half of all investigations that are contracted out by the Office of Personnel Management. The case alleges that USIS sent back to OPM investigation reports that were not yet complete in order to maximize profits, a practice that I previously referred to as "dumping."

For Ms. Kaplan, if I could, this lawsuit comes on top of all the questions that have been raised about the investigations of Aaron Alexis and Edward Snowden. Are we at a crisis point with the credibility and integrity of the security clearance process? What should give us any faith in the current system?

Ms. KAPLAN. I appreciate the question, and I certainly understand it based on the reports that have appeared. As you mentioned, Senator, on Tuesday afternoon, a False Claims Act complaint was unsealed, and it contains very serious allegations of contract fraud against USIS arising out of conduct that took place in 2010 and 2011. We have been aware of these allegations since the complaint was filed in July 2011. We have been working closely with DOJ and our IG to implement changes that would address the contract fraud and ensure that it would not continue.

Let me explain to you what we understand the allegations to be.

We understand the allegations to be that—well, the contractors have an obligation under the contract to conduct their own quality reviews of investigations. Once they finish their quality reviews, they send the product to OPM, and we conduct our own quality reviews of the investigation.

What the allegation is here is that, in order to move cases more quickly, USIS did not conduct its own quality reviews. And that is a real problem, obviously, if the allegations are substantiated because it is contract fraud, because they were certifying that they were completing the quality reviews. It is also a real problem because we rely on their quality reviews in order for us to be able to move the investigations along more quickly. We like them to catch issues and fix them before they send the reports on to us.

I will say, maybe it is cold comfort, but the cases that were, to use the phrase, "dumped" were cases that also were subject to OPM quality review. So it is not that the cases were never reviewed before they were passed on to the agency.

That being said, we have done a number of things as soon as we became aware of the allegations. With respect to OPM, we have significantly increased the number of government personnel performing contractor oversight by increasing the number of people, the full-time equivalent (FTE) levels, and realigning our internal staff.

We have increased onsite inspections with contractor review, including a comparison of their process to the requirements of the contract.

We have increased the frequency of the audits of cases closed by the contractor.

We have developed a new report to detect instances where quality reviews may not have been performed according to the terms of the contract, as is alleged to have occurred here.

We have sort of conducted inspections on the average number of reports being reviewed and released by the contractor's review staff for trend analysis so we can find anomalies.

We have removed former USIS officials allegedly involved with the misconduct from the OPM contract.

And we are currently in the process of recompensing our support services contract, which is also held by USIS, to preclude a concern that there might be collusion between the support staff and the field investigators. And that was a recommendation of our Inspector General.

Lots of things have occurred at USIS since this——

Chairman CARPER. My time has expired. I want to be respectful of my colleagues.

Ms. KAPLAN. OK. Sure.

Chairman CARPER. But just sum it up in one more sentence, and then I need to recognize Dr. Coburn. But thank you. This is a good response.

Ms. KAPLAN. Understood. Well, a lot of changes have been made at USIS. There is a new Chief Executive Officer (CEO) there. There is a chief compliance officer. There are new integrity standards. There is an internal audit committee. There have been a lot of changes made since the events that are revealed in the complaint, and that has given us some level of comfort and confidence that we can rely on these products, rely, and trust, but verify.

Chairman CARPER. Trust, but verify. Well said.

Dr. Coburn, thank you.

Senator COBURN. Well, thank you. Thank you for your testimony. I kind of see this as a multitude of problems. I mentioned in my opening statement we overclassify, which is a problem for the American people because that means it is not transparent. And sitting on the Intelligence Committee, I get to see what is secret and what is top secret, highly classified and compartmentalized.

One of the other things I see is in five different instances we have people who are doing the investigations who are also doing the adjudication. So we had an absolute conflict of interest in terms of separating of authorities and responsibilities in five areas in the

clearance process, five separate areas where we have the same person adjudicating or the same firm adjudicating what was cleared, what was investigated.

Third, as we have noted, we have three different instances in our very remote history where we have obviously failed in terms of our clearances. Whether it is Bradley Manning or what happened here at the Navy Yard or what happened at the National Security Agency (NSA), we have a failure. And the other thing we have is now we know that we have 8,400 people with clearances that do not follow the law when it comes to paying their taxes, and half of them have a Top Secret clearance. The American people ought to be asking what in the world is going on.

So my question is: We have now seen outlined who is ultimately responsible for it. That is the DNI. Correct?

Mr. PRIOLETTI. Yes, sir.

Senator COBURN. And we have the Defense Department that is making improvements but still has a way to go, and we have failure with contractors in allegedly not doing what they are supposed to do. There is also another IG investigation going on along with that. So what is the answer?

One of the answers has to be doing the job that we do better, one. No. 2, the other has to be using data that is available. Where is that form? This form, for 20 bucks you can get 90 percent of the information on the Internet that is in this form. Now, we pay $2,400 for Top Secret clearances. Is that right? That is about what we pay. It is about $2,400.

Ms. FARRELL. For Top Secret, it is more than that. It is a little over $4,000.

Senator COBURN. OK, $4,000. For Secret, what do we pay?

Ms. FARRELL. About $262.

Senator COBURN. OK. And for $20, you can find out 90 percent of this stuff online right now. And so the question is: Maybe we need to step back and say, first of all, we have way too much stuff classified, we have way too many people who have to have a clearance. Second, how we are doing it is not utilizing data that is out there today that is readily available. Third, we have had a response from Director Clapper that they are going to start coordinating with the Internal Revenue Service (IRS). Well, most people would say that is kind of a no-brainer. That would be one of the things you would want to check. You have a form. It is in the form: Have you paid your taxes? But it looks to me like nobody ever cross-referenced that with the IRS. Nobody ever checked to see if that data was accurate. And all that is a computer check.

So I guess my question to you is—and my final point is this: Creating the expectation that your clearance is tentative on the basis of you passing some type of renewal and not knowing when that is going to be—the CIA used to have random polygraph tests. They do not even have random polygraph tests now. You are noticed. I can pass any polygraph test with two drugs in me, and you will never know it. And so the fact is we need to create an environment where, one, we lessen the number of people that need a clearance, we do a whole lot better clearing, and then we need to create the expectation that you are going to be randomly checked to see if, in fact, you still deserve to have that clearance. That is the system.

And the details are difficult. I am not saying it is not difficult. But how we do it and how much it costs and holding contractors accountable for doing the very job we are paying them to do does not seem to be happening.

And my question, I would just like a response from you all: How do we solve this? You all have laid out where we are. But how do we solve it? We have all these areas. This form, three pages of instructions, seven pages where you live, five pages of names, 17 pages of employment, four pages of military, 29 pages on relationship, 21 pages on foreign activity, two pages on emotional health, seven pages on police records, 11 pages on drug and alcohol, eight pages on financial records, five pages on associations, and three signature pages. And I know you are reforming the form, but the point is what we want to do is go for the gold. And so not all of this, first of all, is checked from a quality assurance check, and No. 2 would be: Can we create a process that gets to the gold and not rely on a form as much as we can data that is already out there that the government already holds?

I am amazed—are you all amazed that 8,400 people in this country have a tax debt that makes them vulnerable to divulging secret data or top secret data and they have clearances today? Does that bother anybody here? That puts us at risk.

So my question is: Whoever wants to answer my broad commentary or at least educate me in a different direction, I would love to have it.

Ms. KAPLAN. If I could just make one point, and I am sure my colleagues will jump in. You had noted—and I think this is a misimpression that a lot of folks have—that the contractors are doing both the investigations and the adjudications, and that would be a really bad system. But, in fact, the adjudication is not done by the contractors. It is done by the agency that is granting the clearance. So I just wanted to make——

Senator COBURN. Can they use a contractor to do it?

Ms. KAPLAN. No. That is an inherently governmental function. It is not something we would entrust to a contractor. I believe I am right about that——

Senator COBURN. Let me ask you another question. We are using contractors for this clearance process. To me it would seem that the clearance process in and of itself is an inherently government function, not just the adjudication but the investigation. Any comments on that?

Ms. KAPLAN. Well, I am actually going to turn that over to Mr. Jordan.

Mr. JORDAN. Senator, the collection of information, the analysis is not an inherently governmental function. As Director Kaplan said, the decision, the adjudication is an inherently governmental function. That should only be performed by government employees. But the collection of information is not inherently governmental.

And to your earlier question, this goes to the very nature of what we are doing in our coordinated interagency review. How do we get the right data in the right people's hands at the right time to make the right decision? So Continuous Evaluation, which Mr. Prioletti spoke of, is a very important piece. Automated records checks, to the extent that we can build out our capabilities there, very impor-

tant. Building both efficiency and effectiveness, furthering both of those in the system. And then making sure that we are constantly looking at all of the processes in the end-to-end spectrum, from initiation through the investigation and the adjudication, and then on an ongoing basis to make sure that we address any gaps, any weaknesses as quickly as possible.

We have about 5 million people with security clearances, and you noted several instances, but they are few. The issue is any single point of failure has such monumental negative consequences that we need to do everything we can to make sure we do not have a single one.

Senator COBURN. Well, I have not heard anybody say anything—I think Senator Tester and I agree. We classify way too much stuff. Do you all disagree with that? And what is the answer to that? Because once you create something that is classified, the only people that can work on it are people that have a clearance for that classification or above. What is GAO's response on that?

Ms. FARRELL. That is a separate issue from the people part, but we have done work in the past looking at the potential overclassification of materials, and we do have work that just started looking again at the potential overclassification. That, though, does relate to the first step of the personnel security clearance process, determining if a position needs to have access to classified information, and that is where those types of tradeoffs could be made.

There is a misperception often that security clearance follows the person. It does not. It follows the position, so as we have noted, there has been a lack of guidance in that area. We did work at DOD and DHS, components within both of those departments. We found that some components took initiative to revalidate existing positions, and some did it one time and had no plans to do it again. Some never did it.

So from a personnel security clearance process view, that very first step is very important to make sure that the position does require access to classified information. That is where those types of questions could be asked: What is that classified information? If you overclassify, then you overclassify positions, then it starts the snowball effect of having 5 million people who have clearances now.

Senator COBURN. I will wait for the second round. Sorry.

Chairman CARPER. That is quite all right.

Just a quick note, if I could. I did a little bit of math. I hope I did this right. If there are 8,400 people out of the 4.9 million people that have clearances, that is about 0.16 percent that apparently owe the government some money. My hope is that most of them are on a repayment schedule. We do not know, but hopefully they are.

Dr. Coburn says 40 percent of those are on repayment schedules, so that means that about 0.16 percent owe the government some money that are not on a repayment schedule. That is not good. But compared to what? Compared to the 99.9 percent who have a clearance who do not owe the Federal Government anything on taxes. So——

Senator COBURN. Would you yield for a minute?

Chairman CARPER. Sure.

Senator COBURN. To me it raises the question. It is not about a percentage. It is if you are not following the law in terms of paying

your taxes, why should you have a security clearance at all, whether you have a payment plan or not? You have not complied with what we expect every other American citizen to comply with, and you have a security clearance? To me it begs the question, you are not up to date on your taxes, you no longer have a clearance, period. I mean, it is creating the right expectations, is my thought.

Chairman CARPER. OK. Good. The other thing I would say, I spent 23 years of my life as an active and reserve duty naval flight officer. If I had a dollar for every time I heard me and others of my colleagues say, "We have too much stuff overclassified"—this is an age-old problem. It is still a problem. I would readily acknowledge that. It is the kind of thing we have to go back again and again and again in looking at this stuff that we are classifying and ask the question: Do we really need to classify this? So that is a good question to ask.

Senator Tester, you have done good work, you and Senator Portman there sitting next to you, and Senator McCaskill and others. We thank you for all that, and you are recognized.

Senator TESTER. Yes, thank you, Mr. Chairman, and I think even the bigger issue than the taxes paid is that taxes paid is pretty basic, so what else is going on out there that they are allowing—that are slipping through the cracks on security clearances? Because taxes, I mean, that is right in front of our face, and we are missing that.

Mr. Chairman, to followup with Senator Coburn's comments, I think that we have pushed through this Committee the revolving fund dollars to be allowed for more transparency, more audit, and more accountability. The House Committee has passed that, but the House has not, and I would encourage you to do what you can do with your counterpart over in the House to make sure the full House takes that up, because that is critically important.

Then there are two other pieces of that bill that Senator Portman, Senator McCaskill, Senator Johnson, and Senator Coburn are all a part of, plus some others, that deals with accountability and it deals with a number of clearances that are out there, and I think that we should push to try—I know there are negotiations going on, but you have to set a level of expectation, and I think that is what that does in part.

I want to followup a little bit on what Chairman Carper talked with you, Elaine, on the DOJ suit that was filed in July, 2011, and we were told by OPM that there was not any problems with USIS. And there is a suit out there that does not look very good to me, and now we are finding out that OPM is probably going to get on board or may be going to get board or is getting on board. What is going on? It looks to me like, quite frankly, there is a real disconnect here between what the contractors are doing and what the expectation is for the contractors to do. And people are dying because of it. We are losing critical information because of it. I mean, the list goes on and on.

So what is going on?

Ms. KAPLAN. Thanks for the question. I am not aware of anyone at OPM saying there was no problem with USIS. I do know that because of the fact that this complaint was under seal we were unable to talk about the complaint. And now we can talk about the

complaint, which I think is a good thing. And I think what we have tried to do, as I was explaining to Senator Carper before, was—and this started before the complaint became public, and it has been over the last several years—is to address and to rectify the problems that are revealed in these allegations in this complaint, which was under seal.

And as I mentioned, we have done many things at OPM to prevent this from happening again. This is contract fraud, a failure to do quality reviews that they were obligated to do under the contract. And there have been many changes made at USIS as well—many changes involving a whole new staff at the top, a compliance office, internal audit, all sorts of things that have given us greater confidence——

Senator TESTER. When were those changes made?

Ms. KAPLAN. Those changes have been made over the last 2 years, since the allegations in the complaint, and we have been working with our IG on it and with the Justice Department, and so we feel that the allegations are certainly very disturbing, and what we have tried to do is address the underlying concerns without speaking publicly about them.

Senator TESTER. I am not an attorney, but they have been sealed, but you have known what is in the charges, you just cannot talk about it publicly. Is that correct?

Ms. KAPLAN. I can tell you right now—in fact, you can go online probably——

Senator TESTER. Yes, I do not care about now. I want to know about July 2011. Were you guys aware of what the charges were?

Ms. KAPLAN. We knew what the allegations were in the complaint. However, working with the Justice Department and our IG, we were advised, of course, not to discuss it because it was a matter under seal.

Senator TESTER. And that is cool. That is fine. I guess the real question here is that they—USIS does 60 percent of the background checks, right?

Ms. KAPLAN. I think it is 50.

Senator TESTER. 50 percent, which is——

Mr. KAPLAN. Yes, close enough.

Senator TESTER. There are three companies that do the contracting, so they are doing the lion's share of it.

Mr. KAPLAN. Yes.

Senator TESTER. Was there any oversight, additional oversight given as of July 1 on the work that they were doing? How often was it done? And, by the way, are those kind of metrics used now on all of them? Because, quite frankly, when money is involved, obviously there are some folks that do not give a damn about the product and they just want to make the money.

Ms. KAPLAN. Yes, I mean, that is a good question. What we have done—and it is not just oversight of USIS, because we have other contractors and we have Federal employees, quite frankly, who do the work, too. They need to be watched.

Senator TESTER. So what determines what background checks go to USIS and what goes to—these guys do some things particularly well and other things not so well? Or do you just dole them out like a deck of cards or what?

Ms. KAPLAN. I do not think it is like a deck of cards, and I actually do not know what the—I will get an answer to you on that question. I suspect it is based on the location of the investigation, but it is not as though, oh, they do the top secret and the Federal staff does——

Senator TESTER. I believe it was you that talked about quality metrics. It might have been Brenda, too. What determines what background checks you guys look at to see if they are done appropriately?

Ms. KAPLAN. We look at all of them. We look at each background investigation.

Senator TESTER. So you looked at Alexis' background check?

Ms. KAPLAN. Yes, we did. Well, would you like me to talk about the Alexis——

Senator TESTER. Well, I mean, you can, but the information is out there. I mean, the naval record alone should have brought up some red flags.

Mr. KAPLAN. Well, what we did——

Senator TESTER. And what you are saying is two folks missed it now. USIS missed it—well, I do not know if USIS did that one or not. But the contractor missed it—they did?

Senator MCCASKILL. They did.

Senator TESTER. The contractor missed it and you guys missed it.

Ms. KAPLAN. Well, to be clear, I would have to say that based on our own review and I believe also ODNI's review the Alexis investigation, yes, we all missed something for sure. But we did what was required of——

Senator TESTER. Multiple somethings.

Ms. KAPLAN. Well, I want to make sure, because it is really important to get to the root cause of this, that we understand each part of this. We did the investigation in 2007, and it was for a Secret clearance, and there are certain protocols and standards that apply to a Secret clearance. It is not a Top Secret clearance. We conducted the investigation that was required by the Investigative Standards, so having gone through quality control both at USIS and OPM, we would have passed that investigation because it complied with Investigative Standards.

Now, what we are looking at right now in the context of the review and what we have been looking at is, well, are the standards up to snuff? Should we be required to get police reports, for example? Should we be required to get mental health information even from someone who has a Secret as opposed to a Top Secret clearance? All these things need to be looked at. But it was not, in our view, a case of malfeasance on the part of the contractor. We believe the contractor did what they were supposed to do.

Senator TESTER. Senator Coburn obviously knows what you looked at because he had the thick file, but if you do not look at police reports and you do not look at criminal background—what do you look at?

Ms. KAPLAN. No, we did look at the criminal—I will tell you what we looked at. The way it works is when—with this Secret clearance is that there is an FBI check done, and we get the FBI database, and the FBI reveals arrests, it frequently does not reveal the dis-

position of cases that are handled at the State and local level. And so the FBI record revealed that Mr. Alexis had been charged and arrested for what was called "malicious mischief." And under the existing standards, our job, or the job of the contractor in this case, was to go out and find out what the disposition of that charge was and to find out more information about the charge.

Now, some have questioned now why OPM's investigators did not go get a police report. Well, the reason that a police report was not obtained was because , there were like 1,700 different localities, law enforcement jurisdictions. They all have different rules about what they are going to supply to us. And in this case, we had experience with Seattle. Seattle did not provide police reports. And they have their own good reasons, I am sure.

Senator TESTER. All right.

Mr. KAPLAN. So what we were referred to by Seattle was this State database, the State of Washington, their court records, and that is where we went. And that revealed that Mr. Alexis was charged with malicious mischief, but the charges were not——

Senator TESTER. Can I—and I appreciate I am over time, but can I just ask you, when you guys do an oversight look, how many do you find a problem with?

Ms. KAPLAN. I do not have that information, but I can get it for you. If there is a problem—and there are all kinds of different problems—we try to get the contractor to fix the problem, for example, if it is incomplete. And then if there is a problem, if the adjudicator looks at our investigation and feels like it is inadequate, they can come back to us and ask us to do more work.

Senator TESTER. We could be here all day, and we probably should be here all day. It is important. Thank you.

Chairman CARPER. Thank you, Senator Tester.

Senator Ayotte, welcome.

**OPENING STATEMENT OF SENATOR AYOTTE**

Senator AYOTTE. Thank you, Mr. Chairman, and I want to thank you for holding this very important hearing.

Let me just followup as to what Senator Tester said. As I understand it, in the case of Mr. Alexis, OPM did actually go to the Seattle Police Department to get the underlying police report?

Ms. KAPLAN. No.

Senator AYOTTE. They did not?

Ms. KAPLAN. No, we did not because we do a lot of these investigations and our understanding was that Seattle did not make that kind of information available. They routinely referred us to the State of Washington database, and that is where we went.

Senator AYOTTE. So we did not try to get the underlying police report. The decision of OPM was just that we have dealt with Seattle in the past, they will not give us a report?

Ms. KAPLAN. Well, our obligation is to try to find out the disposition or if there have been charges, and it was not as though we decided we are not going to make an effort here. We just, based upon the fact that in the past—and this occurs with other jurisdictions besides Seattle. They will refer us to another database, and, that is what they did. And we did not go in this particular case and say, "Will you depart from your policy?" But, just—this is, again, some-

thing that we need to take a really close look at and we are going to be looking at as part of the President's review, because it is problematic, certainly, that, there was this information written on a piece of paper somewhere that we did not have access to.

Senator AYOTTE. Yes, I find it actually incredibly shocking that we would not pursue a police report in any of these arrest situations, because the nature of the charge looking at the underlying police report, having been a prosecutor, can tell us very different information, and a prosecutor may not have the elements to make a particular charge, and the disposition may tell us nothing. But, seeing prior behavior here with Aaron Alexis getting a police report would have flagged a very different set of conduct for anyone looking at that. So I believe we do have to change that, we do have to get the underlying reports. And if that requires coming to an understanding with law enforcement across the country, I would be shocked, having worked with so many police officers, that they would not be willing to have an understanding with the Federal Government on this given what is at stake for the country.

One of the things that concerned me also as I heard the discussion, Judge, between you and Mr. Tester was this issue of the USIS lawsuit. In 2011, coming before the Committee, I was not a Member of the Committee then, but the fact that this suit was sealed and as a result of consultation with Justice you did not feel because of the sealing of the suit that you could share that information. I understand you have to go to Justice for advice on these issues, so I am not being critical of you on this. But what I would be critical of is why wasn't there—this seems to me a core issue of oversight that the Committee would need to know that was the subject of this sealed suit that now we are seeing obviously some of the consequences of perhaps part of this being USIS obviously with Snowden and with what we are seeing in other cases. And it really troubles me to think that this would be sealed. Was there any discussion with Justice about how this is a very important piece of information that the Committee really needs to know? Because I have a real problem that Justice would not have gone to the court and taken actions, having been a prosecutor myself, to try to unseal it, explain that there is a separate duty here that the Congress needs to be aware of information and protect the country. And I think this is part of a bigger issue, so I wanted to get your thoughts on that. And did you come subsequently and update us as soon as you could once this thing was unsealed?

Ms. KAPLAN. I am here today. It was just unsealed 2 days ago.

Senator AYOTTE. OK. Fair enough. So, in other words, it was sealed for 2 years.

Ms. KAPLAN. Well, and, I am not an expert in this, and thank you for calling me "Judge," even though I am not a judge yet. I appreciate it. And I am not an expert in this, but this is, a False Claims Act case——

Senator AYOTTE. Right.

Ms. KAPLAN. They are—they have a very special treatment because somebody comes forward as a whistleblower, and then the government has to keep it under seal because the government wants to decide whether to intervene in the case.

Senator AYOTTE. Right.

Mr. KAPLAN. And so I think that is the reasoning behind the sealing. That is——

Senator AYOTTE. So understanding that there obviously are different rules in a False Claims case—but this is an issue because we have a separate responsibility, and we have to get to the bottom of this so that this Committee is not waiting a couple years later while this decisionmaking is ongoing in the Government when there is a critical issue with a contractor that needs to be addressed. I believe that this is an important issue that we have to get at.

Senator COBURN. If you would yield, I think the real question is, now that you have this problem out there, the response I would say is: Why weren't we monitoring quality assurance on our contractors to begin with? And what have we done since then to monitor quality assurance on the three contractors that are out there doing it?

Ms. KAPLAN. That is a fair question. With respect to what were we doing before, I have been told that actually we were sort of hot on the heels of this around the time that the complaint was filed, because we were starting to notice that the quality reviews were being done either too much by one person or too quickly, and so we had already made inquiry with USIS. But obviously we did not catch it quickly enough, because it occurred. And so what we have done since then is we have focused more, as I had said before, on those reports to enable us to find anomalies before the problem was occurring more quickly, and we have beefed up the staff, the Federal staff that is working on those matters. And at the same time, USIS has made many, many significant changes in the way that they operate, and so there have been a lot of changes made.

And with respect to the question about not being able to talk about it, in some ways it was very frustrating to us as well, because you are looking at——

Senator AYOTTE. I can imagine.

Ms. KAPLAN [continuing]. Things in the newspaper and you are unable to—but I think that you would have to ask the Justice Department more about it, but I think that they believe that this is required by law.

Senator AYOTTE. Thank you. And I think obviously that is something we need to work through so we are not in this situation in the future.

I also wanted to ask about—I believe, Mr. Prioletti, you raised the issue of Continuous Evaluation, and yesterday Senator Collins, along with Senator McCaskill, myself, and Senator Heitkamp, introduced a bill that would provide—one of the issues I see in all of this is an issue that we rely too much on self-reporting, particularly after we have granted a clearance. And our bill is fairly straightforward in that there would be two random audits conducted.

As I understand your testimony, you have talked about this idea in your testimony of automated record checks, yet you say there is more research required. I do not understand how, if we do not have some random checks and we are relying totally on self-reporting—frankly, people's lives change dramatically and can change in 5 years' time—that we will have a system that really verifies that

people should maintain their clearance status. So I wanted to get your thoughts on that.

Mr. PRIOLETTI. Thank you, Senator. What I was referring to is we do automated record checks at this time or electronic record checks. All the government agencies do that at times. For example, when Director Kaplan referred to the police checks, going to the electronic record checks to get that information, there are ongoing processes such as that going on right now.

What I was referring to with Continuous Evaluation is an expansion of that into more areas that include internal government databases as well as external, both government and commercial databases. Some of the specificity I cannot get into in today's current environment in this proceeding here. But what we are talking about is building the enterprise-wise—in other words, have an automated records check ability, a Continuous Evaluation, whether it be several times over a 5-year period or whether it be more frequently than that, that can serve both the United States military units, can serve the intelligence community as well as serving the non-Title 50's.

What we have done is we launched a CE, if I may use the term, Continuous Evaluation Working Group that was made up of Intelligence Community (IC) members, OMB had representation, OPM had representation, and DOD had representation. And we created a concept of operations that is now ready for testing that takes a level of checks that are high enough to satisfy the requirements of Top Secret Sensitive Compartmented Information (SCI) organizations such as the IC, but also reasonable for the expectations of an non-Title 50 organization or some of the other organizations. That is a very touchy balancing act to make sure that we have enough checks, but it is an expansion on what is currently done.

Director Kaplan mentioned that there are national agency checks, police checks, and financial checks for the Secret level clearances. We have expanded those to cover other areas, some databases which include classified information and some that do not, as well as the commercial databases.

The area that I think you are most concerned about is the social media or publicly available electronic information, and that is where the research is being done, Senator. We have to find that balance between the civil liberties and privacies of a U.S. citizen versus national security interests. That is where we are doing it. I do not have, as a representative of the ODNI, the luxury of going into a social media or publicly available database, pull information out of there, and submit it as being the truth. The government has a responsibility, an obligation to every one of its citizens to ensure that the information is true and accurate before we use it in the adjudicative process.

Senator AYOTTE. Well, I know my time is up, but I can tell you that obviously when our teenagers go online and get important information on social media and yet we are not going to use it to find out that someone is involved in something, I think that is a little hard to believe. We need to take a commonsense approach to this.

So my time is up. I also think we need to have random checks on people instead of just relying on their own self-reporting. Thanks.

Chairman CARPER. Senator Ayotte, thank you. Senator Heitkamp.

**OPENING STATEMENT OF SENATOR HEITKAMP**

Senator HEITKAMP. Thank you so much, Mr. Chairman, and thank you, Ranking Member. I think this is such a critically important response and quick response to this horrible tragedy, and I hope that the family members take some comfort that we, too, share their concerns.

I have read this report, and I can tell you honestly, as somebody who used to do background checks for people involved in gambling in North Dakota, if you were going to get paid minimum wage to deal Blackjack, he would not have passed that background check. He could not have dealt Blackjack in North Dakota, but yet he had a clearance that allowed him to come on to a Navy base and do serious human damage. And so it is really frustrating; we are all frustrated here with this process.

And I completely appreciate your privacy rules, but when you apply for this clearance, you waive your right to privacy. And every parent on this panel who deals with social media knows if you want to know what your kid is doing, go out on social media. You may think that does not have the veracity of a court record, but I can tell you, as somebody who has looked at court records repeatedly doing background checks, it certainly does. A picture is worth a thousand words, and it is heartbreaking.

And so we take this one example, and I always fear that one example does not prove the case, but we have multiple examples now of where we failed in the clearance system to actually ferret out people who would do damage to co-workers, murder co-workers, but also damage to our national security. And so this is a very broad issue and a very important issue.

I want to talk about self-reporting, and I want to talk about the consequences of not self-reporting. I was, quite honestly, shocked—because I am new to this Committee and new to looking at government security clearances—the huge number of people in this country who have these clearances. I mean, this is a big group to manage. Right? We would all agree with that. So obviously random checks are a critical and important part of this, and you see that from the bill that we introduced. But we need to make the self-reporting more effective as well.

So I want to know, of all those millions of people who have these clearances, how many have ever been discharged from the government for failure to self-report.

Mr. JORDAN. We can get you that information. We do not have it with us.

Senator HEITKAMP. In your database, how would you know that information?

Ms. KAPLAN. Well, if, for example, someone fails to report—do you mean on their form they are deceptive and they——

Senator HEITKAMP. No. Either lying on their application or failure to report after a serious event that occurs after the clearance.

Ms. KAPLAN. We will have to get you that information, but the latter is certainly grounds for revoking a security clearance, and failing to report or being dishonest when you fill out your form is

something that the adjudicator would take into consideration in deciding whether to grant a clearance in the first instance.

Senator HEITKAMP. Right, but if you are—with all due respect, if you are not checking local police records, you have no guarantee that when somebody checks the box and says they have never been arrested, they are telling the truth.

Ms. KAPLAN. No, and with respect to that, there is never a guarantee, but we do not just take their word for whether they have been arrested. I mean, we do an FBI check, and the FBI database, which receives reports from the States——

Senator HEITKAMP. I am familiar with it.

Ms. KAPLAN. Yes, probably more familiar than I am, frankly. It will spit out whether someone has been arrested, and then we do the followup, and it often requires work on a State-by-State basis or local jurisdiction to find out what the disposition was.

Now, let us remember, we are talking in his case about a Secret clearance. If it was a Top Secret clearance, there would have been a more extensive investigation done, which perhaps would have uncovered the gun part of this and maybe other things. That is speculation, but this is a Secret clearance.

Senator HEITKAMP. If I can just take it one step further, we are talking about revoking the clearance. What about requiring that employment be terminated? Is that one of the things that you are considering and looking at going forward, that this person obviously—for contractors that is a tough call. But certainly for government employment, to me it is not enough to just revoke their clearance. I think that it should be prima facie a case that you now lose your job.

There has to be serious consequences for not reporting. There has to be serious consequences for lying. And we have to look at the number of people who are out there who are not currently self-reporting, because even random checks cannot solve this problem. There has to be true consequences. And so I am interested, anyone on the panel, about how we are going to amp up the penalties for employees not self-reporting.

Mr. JORDAN. That is absolutely what we are looking at as part of our 120-day interagency review, both the piece that you were talking about where, are there any gaps in the self-reporting portion versus an active reinvestigation period would address that in scope. What is the information that we collect and measured against the 13 adjudicative standards, and does it all flow right? That is all part of it and then the accountability. There are currently significant penalties for lying or not reporting adverse information. Yes, it includes revocation of your clearance. You mentioned contractors. An agency can suspend or debar the contracting firm. If they think it is just a problem with an individual, they can direct that that individual not work on that contract, or you could suspend or debar the individual. And we are looking at all of the accountability measures for both Federal employees and contractors to make sure that only the people who should have access to our facilities and our sensitive information do at any given time, not just when they are cleared.

Senator HEITKAMP. Yes, I mean, just human nature being what it is, if simply saying, well, there might be a consequence or—the

point that I am getting at is a mandated: this is going to happen if you do not self-report. And, Mr. Contractor, we do not know this; it is your job to help us enforce, it is your job to report back to us. And if you do not, black mark on you, you will not be a government contractor very long.

And so that is the level at which I have passion for this issue, that we should not be letting—when we give them the Good Housekeeping Seal of Approval, which is what this security clearance is, that ought to mean something. And if they breach it, that ought to be something that we consider very serious with very serious consequences.

And so I applaud your work. I would like to know how many have actually been discharged or disciplined for either lying on applications—obviously they would not get the clearance, but not reporting after the fact.

Mr. Chairman, again, thank you for the time.

Chairman CARPER. Thanks for those tough questions. Senator McCaskill.

**OPENING STATEMENT OF SENATOR MCCASKILL**

Senator MCCASKILL. I think one of the most revealing things this morning is the realization that while an arrest report may be part of a background check, there is not a requirement that the underlying police report be obtained. And I will tell you why this is a shocking revelation. Like Senator Ayotte, I am a former prosecutor, and the vast majority of cases that would reveal a mental disturbance will not have a disposition.

The criminal justice system does a very bad job of adjudicating the mentally ill because with the mentally ill really, from a prosecutor's standpoint, if they have not hurt anyone, putting them in prison sometimes creates more problems than it solves. So most prosecutors, when they are confronted with a mental illness issue, like someone who says they have heard voices, someone where the police have been called to a motel room on a disturbance where someone says there are microwaves coming through the vents and, "People are here to get me," they will do a police report, and most of the time the police department will not even try to file charges. That is a disturbance call that is related to someone that, in their minds, they do this all the time.

Now, that is not something that—especially in a city as large as Seattle, Kansas City, or a city as large as St. Louis, that kind of disturbance call, where someone is making a racket because they are mentally disturbed, most police departments will not even take it to the prosecutor for disposition. In fact, we are horrific in this country with even getting that person to mental health services. And the vast majority of these shootings are not going to be around the issue of whether or not someone has shown violent tendencies but whether or not they have shown tendencies of having a mental issue.

So the notion that we are saying, well, if a police department will not give us the report, we have checked the box, and I think if we do a gut check on this issue, we will realize that a lot of the work that we have been doing around this has been checking boxes.

Now, I get it that we cannot go out and do one-on-one and pull every thread on every application for clearance, although if we did that, we would probably make them so expensive, we would be much more disciplined about deciding who gets them. But the notion that you are calling what you are doing quality control, Ms. Kaplan, is probably, I think, offensive, because I think there is just a lot of checking boxes going on. Was this report obtained? Yes.

What I do not have confidence of is that there is, even on a random basis, a more thorough examination. And I am glad to hear you have a working group, and what I would like to see us do as a Committee is ask for some specific recommendations on who is getting clearances and are they all necessary. And all of this is risky. I mean, we can say that we are doing too many, and then we could have a bad thing happen. And then we would be back here saying, "Well, why didn't they have a security clearance?"

On the other hand, what we are doing now is the worst of all situations because we are giving the impression that all these millions of people who have security clearances, we have checked them out. We are confident that they are mentally stable, they are not criminals, and they obey the law. We have no idea if that is true. We are clueless as to whether or not that is true, because this process has become in a way a pro forma kind of process with contractors. And the reason the contractors were off the reservation is because they bid an amount and that contractor wanted to make money, so that was time to cut corners. You wanted to make your number? You wanted to make money? Well, then, you did not have to do the whole thing. You just turned it in and pretended like you did.

So I agree with the Chair and the Ranking Member that this is time for all of us to really quit nibbling around the edges on this thing and let us get to the meat of the matter. Saying that Seattle does not give a police report, that dog does not hunt in this context. That just does not work.

And, Mr. Lewis, I have a specific question for you. My Subcommittee has learned that we have had a bunch of felons on Navy installations. We have learned that the Navy was giving these contractors 28 temporary passes at the get-go without any checks on anybody. Is that true?

Mr. LEWIS. This was a subject of a DOD IG report, and the Navy has looked into these specific circumstances. I believe there were about 50 people identified who were convicted felons who were given access without the proper checks, and the Navy has taken corrective action, removing individuals who do not warrant access from the installation.

In other instances given the date that—some of the felony convictions were quite old, the Navy made a decision to allow them to continue to have access.

But the fundamental issue is there was a failure to conduct the required checks for installation access, and the Navy has taken corrective action on that.

Senator MCCASKILL. And so no more temporary passes?

Mr. LEWIS. The passes would have to be based on the required checks, the National Criminal Investigative Check as well as the terrorism database check.

Senator MCCASKILL. OK.

Mr. LEWIS. So that would bring up a felony conviction.

Senator MCCASKILL. OK. So is there a different status for a certain kind of pass than for a permanent pass now? Are you saying that they are doing something before they do a temporary pass? Or are they getting the full complement of checks?

Mr. LEWIS. For installation access, there are two basic criteria. One is someone who is going to be on the installation on a temporary basis. Those individuals require a degree of vetting, a criminal records check and the terrorism database check. For individuals who are going to have ongoing access, there is a requirement for a national agency check with written inquiries and other checks, which is the minimum standard for that CAC issuance.

Senator MCCASKILL. So we have corrected the problem that someone was getting temporary passes without any check.

Mr. LEWIS. Yes.

Senator MCCASKILL. And is this going on in other branches, temporary passes with no checks?

Mr. LEWIS. We are not aware of that, but we are certainly engaged with the components on this particular issue.

Senator MCCASKILL. OK. Well, I would like a report back that this is not going on in any of the other branches.

Mr. LEWIS. Yes, ma'am. We will do that.

Senator MCCASKILL. Thank you. My time has expired. Thank you, Mr. Chairman.

Senator COBURN. Just one followup, just for information. Who ever made the decision to allow that to happen, to go around? Were there any consequences to that individual that actually made the decision?

Mr. LEWIS. There is an ongoing Navy review of what occurred at the Navy Yard that day, to include all of the aspects that went into that, and that is an ongoing review.

Senator COBURN. Could we hear back from you to this Committee when the review is completed as far as the consequences to the person who made that decision?

Mr. LEWIS. The Navy review, the overall DOD reviews, and other reviews that are being conducted will be brought together in an OMB final review of our overarching security practices, and I expect that to be part of the review.

Senator COBURN. Well, my specific question is a report back to the Committee on it; somebody was held accountable for going outside the curve. That is a real problem, is accountability in Federal Government. It is accountability. And all I want to know is what are the results of holding some—did we hold whoever made that decision accountable?

Chairman CARPER. I would appreciate it if you could just close the loop at the end of the day for us, if you would please.

Mr. LEWIS. Yes, we will do that.

Chairman CARPER. Thank you.

All right. Senator Portman, please. Welcome.

**OPENING STATEMENT OF SENATOR PORTMAN**

Senator PORTMAN. Thanks, Mr. Chairman. I appreciate your holding the hearing, and I think it has been constructive because we have raised obviously a lot of troubling issues and had the opportunity to hear from some Senators who have a lot of interest and background in this.

At the Federal Workforce Subcommittee, as you know, we have held some hearings, and in June we held one regarding background investigations, and specifically the inability of the OPM Inspector General to effectively audit the revolving fund and really the background investigation process. And that is why the SCORE Act was developed—Senator McCaskill is still here, Senator Tester, and the Chair and Ranking Member and others. And I am pleased that we were able to get that done. Just a couple weeks ago we got it off the Senate floor. It is a small step, but it does fix that IG issue. And I know, Brenda, you worked with us on that, and we want to continue to follow that and make sure we get that cleaned up.

We have another hearing in a few weeks to continue looking at this issue and others, and Senator Tester, who again was here earlier, we are going to stay on this at the Subcommittee level.

I am going to focus on something that I think is critical if we are really going to get at this issue, and I guess the tragic example recently at the Navy Yard is unfortunately a perfect example of it. But it is not a new issue. It is this whole issue of continuous evaluation, and, whether it is the 5-year cycle or the 10-year cycle, this is to me the critical issue that we are missing. And we saw it not just with regard to the Navy Yard, but also with this Ricky Elder case. This is the specialist, Ricky Elder, who, in 2012, shot and killed his commanding officer at Fort Bragg and then turned the weapon on himself. His clearance timeline was actually reminiscent of Aaron Alexis'. His background investigation was done in 2006. Over the next 5 years after 2006, he was charged twice with assault, once for DUI hit-and-run, once for felony aggravated assault—by the way, none of which were reported in his personnel security chain.

Aaron Alexis, similar: After receiving a security clearance, he received nonjudicial punishment for unauthorized absence while in jail for disorderly conduct; another nonjudicial punishment for being drunk and disorderly; an arrest for firearm discharge; multiple law enforcement interactions, both military and civilian, a month prior to the incident that would have highlighted his mental health problems. And none of these triggered a reevaluation of his access to classified material, classified facilities, none of those.

I think this is—I mean, every issue that was raised here today is important, but if we do not get at this, this interim period between a clearance and—again, whether it is a 5-or 10-year cycle—the next clearance, I think we are going to continue to have these tragic incidents.

In 2005, interestingly, a year before Ricky Elder enlisted in the Army, 2 years before Aaron Alexis enlisted in the Navy, and 7 years to the day before Ricky Elder's deadly attack, the Department of Defense testified to this Committee—and this was in June 2005—about the Automated Continuous Evaluation System, (ACES). And you all said that you were going to continuously

evaluate the background and suitability of security clearances. Mr. Prioletti, in your opening—in your written statement—I did not hear you say it in your statement, but in your written statement you noted that 3 years earlier, in 2008—3 years later from the 2005 testimony you gave before this Committee, in 2008 President Bush directed by his Executive Order that an individual who has been determined to be eligible for or currently has access to classified information shall be subject to Continuous Evaluation. That was an Executive Order back in 2008.

I know we have heard today, "We are working on this." I heard in response to an earlier question, "We have an interagency working group. We are developing a concept of operations." I wrote this down. "We are doing research." Again, this has been going on now for a decade. If you testified in 2005 it was going on in 2004, it may be more than a decade.

So here we are. It is 5 years after the Executive Order, 8 years after this Committee heard about the plans, and we are dealing with the tragedy at the Navy Yard.

So I do not know who would like to talk about it. Mr. Lewis, maybe you can talk about DOD. And, by the way, you are also talking about putting something in place but not for another 3 years. And then it would be DOD only.

So I guess I would like to hear what is happening, and, Mr. Lewis, again, since DOD is taking the lead on trying to get this in place, I see from the technical report on the project that there have been some pilot projects. You have 3,600 personnel records that have been searched. And it is working. Sixty-five of those 3,600 ended up having clearances suspended or revoked due to derogatory discoveries. Your search algorithms have found problems. But 3,600 people is a drop in the bucket when we have over 5 million people with security clearances.

So, again, it has been 10 years since we were told, this Committee was told, and I quote: "Beta testing results and lessons learned are being incorporated into an initial operating capability basis to be in place by the end of 2005." And here we are in 2013.

So taxpayers have paid $11.6 million for this just in the 2 years between 2012 and 2014. I do not know what the development costs are—we are trying to find out—or the costs after 2014 to fully demonstrate its capability at DOD.

So can you explain the reasons why this capability will take over a decade to field? Can you give us some sense of the total cost for this and what it is going to cost to field it over at the Department of Defense?

Mr. LEWIS. I cannot speak to the total cost. I would have to come back with that information. But I can give you a current status of how the Automated Continuous Evaluation System is being used. It does provide on-demand queries of a large number of government and commercial data sources, as well as an analytical capability to flag issues of concern. So that is an existing capability.

As you mentioned, it was used in an Army project, and out of 3,300-odd individuals, a total of 100 personnel actions were taken as a result of information identified during those queries.

In addition, the Defense Security Enterprise is developing a Continuous Evaluation concept demonstration which would take this a

step further. So ACES, does a one-time snapshot-in-time query. This concept demonstration would have real-time updates so that as information became available, it would be pushed into the system. And the concept demonstration is currently scheduled to run from April to October 2014. The anticipated population would be 100,000 cleared military, civilian, and contractor personnel. And so we are anxiously looking forward to completing that concept demonstration.

In the interim we are using ACES for Continuous Evaluation checks, again, testing the concept, getting more validation, looking at things like privileged users and some other groups of contractor employees.

So this is an ongoing effort. We get results on a regular basis. And we are looking to take that to the next level in terms of a true Continuous Evaluation, which would give feedback to the system as it is developed so that if an individual gets arrested tomorrow, the system would push that back to DOD instead of waiting for DOD to make that query.

Senator PORTMAN. You were not here in this job 9 years ago when we heard that it was going to be in place by 2005. But you are here now, and so, one question I could ask you is: Why has it taken so long? And you might say, "I do not know. I was not in charge." But you are in charge now, and you are saying that you are going to have this fully operational in 3 years. Is that correct?

Mr. LEWIS. For the Automated Continuous Evaluation System as it currently stands, it is an operational system. It is still in a research and development mode, but it is an operational system. The limits right now——

Senator PORTMAN. I mean, when I say "operational," I mean it actually would cover more than a small percentage of the people who are in between their clearances. You are talking about taking it from 3,600 up to 100,000. How many security clearances do you have at DOD?

Mr. LEWIS. We have about 2.5 million people who are eligible and in access for classified information.

Senator PORTMAN. So when are we going to cover these people?

Mr. LEWIS. One of the things we are examining is can we expand the capability of the system to handle that larger volume, and that is a work in progress and something that we could report back to you on.

Senator PORTMAN. Do you think it is important?

Mr. LEWIS. Yes, we do. We need to address what happens between investigations, and——

Senator PORTMAN. So what are you looking for in order to get this done? You are going to get back to us as to what the costs are.

Mr. LEWIS. Yes.

Senator PORTMAN. Have you sought additional funding? Is that what you are thinking is the problem?

Mr. LEWIS. It is a question of having the right criteria in place to conduct the evaluations and then what we do with the data once it is generated from the system, how you evaluate that and how you take action based on that information.

Senator PORTMAN. My time is up, and I apologize, Mr. Chairman. I just think we have to have some answers on this because if we

do not fix this problem—the initial clearances is incredibly important. We have talked a lot about the need to have arrest records and so on. But if you have this interim period where you are not keeping up with what is happening, and in the case of Aaron Alexis, I mean, it was clear as day, and yet there was no system to incorporate that data. And so to Mr. Prioletti on the intel side, I want to hear what you are doing, too, but we do not have time to get into it right now with this question, but I hope you will get back to us in writing as to what you are doing because we were just talking about DOD here.

And then, finally, I hope that GAO can help us on this to establish some metrics, let us come up with a timeline that makes sense. If you are looking for additional resources or something, let us know. But, if it is going to take another 10 years because we are doing more pilots and more research and so on, that is unacceptable.

Thank you, Mr. Chairman.

Chairman CARPER. Thank you, Senator.

Senator Coburn, and then I will wrap it up.

Senator COBURN. Mr. Jordan, can you explain to me the difference in the field work contract and the supply services contract you have with USIS, one?

And, No. 2, are contractors completing background investigations, then other contractors validating the completeness of those investigations? And are these contractors from the same company?

Mr. JORDAN. So I can answer the second part, but OPM is better suited to answer the first part since they have that contract. And, yes, contractors perform background investigations, and, yes, contractors can perform quality reviews on those investigations. But only government employees make a determination as to whether to grant a security clearance to someone.

Senator COBURN. But my question is: Is it the same company that is validating the work of their colleagues doing the investigations? Is that correct?

Mr. JORDAN. I would have to defer to OPM.

Ms. KAPLAN. No. The companies that are doing the investigations have an obligation under the contract to also do a quality review. But then we do another quality review, and the purpose of their quality review is we would like them to catch errors before the file gets to us, but we do a quality review as well.

Senator COBURN. So OPM is the final validator of the completeness of the investigation?

Ms. KAPLAN. To some extent. I mean, I think another thing that validates the completeness of the investigation, it gets sent to an adjudicator. An adjudicator may want more information. And so ultimately it is a collaborative effort. They may send something back to us. But we are the arbiter of whether we have provided an adequate investigative product, a quality investigative product.

Senator COBURN. Is every investigation validated by you?

Ms. KAPLAN. Every investigation is reviewed for quality, yes.

Senator COBURN. By OPM?

Ms. KAPLAN. By OPM.

Senator COBURN. All right. I have one other question, and then I will submit the rest of my questions. There is a revolving fund

where you charge agencies for this. It has $2 billion in it. Has it ever been audited?

Ms. KAPLAN. I am told it has not by the Office of Inspector General (OIG) because they have told us they do not have the resources, which is why we are supporting, the administration is supporting their request to be able to draw from the revolving fund in order to give them the resources they need to do that.

Senator COBURN. OK. Thank you. I will have questions for the record.

Chairman CARPER. OK. I suspect you will have a number of questions for the record. We thank you for your verbal answers today.

I want to telegraph my pitch. Right now at 12 o'clock in the Senate, we have a new Senator being sworn in. Cory Booker is taking the oath of office, and we will start voting and have the first of several votes beginning about 10 after 12, so we will wrap up here probably about 12:20.

The last question I will ask each of you is this, so you will have a chance to think about it. Sometimes I say when you see something awful that has happened and you hope that some good will come of it, sometimes it does and sometimes it does not. Few things could be much worse than losing a loved one, and 12 families lost loved ones in the Navy Yard, not far from here. They would like to know that something good is going to come out of something that was awful for them, and I think the American people feel that way as well.

One of the last things I will ask you to do is just to reflect on what you said, what you have heard here today, what you have been asked here today, and see if you can give those families some assurance that out of the tragedy they have suffered through, some good is going to come and what that might be. So just know that question is coming, OK?

Senator COBURN. I have one more question.

Chairman CARPER. Dr. Coburn.

Senator COBURN. I just wanted to followup. I am not clear. When you say OPM validates, do you use a contractor to validate?

Ms. KAPLAN. The Federal employees who validate——

Senator COBURN. It is all Federal——

Mr. KAPLAN. When you say "validate," we do a quality review. It is all Federal employees. They do a quality review, too, but then we do one as well.

Senator COBURN. OK. So it is all Federal employees that do a validation on the background information on everything that comes in.

Ms. KAPLAN. Yes.

Senator COBURN. OK. Thank you.

Chairman CARPER. I want to come back, Mr. Prioletti, to—I think a question was maybe asked by Senator Ayotte and I think by Senator Heitkamp, and I want to give you a chance to respond to it. I think it dealt with using social media in the Continuous Evaluation program. Could you just give us some thoughts on that briefly, please?

Mr. PRIOLETTI. Yes, Senator, I can. What I was referring to there is we are seeking to provide as much of the comprehensive capabili-

ties as possible in the overall background investigation on the individual. The more information we can gain, the more enlightened the decision can be on whether or not to grant the access to classified or access to a sensitive position.

One of the obvious sources, potential sources of information, is social media or publicly available electronic information. What I referred to in terms of the research was the idea that we need to look at both what possible sources of information are out there, which ones would be of most benefit to provide adjudicatively relevant information for the access to classified information, and how do we do that in the best way that protects both the personal rights of the individual as well as the veracity and the coverage of the U.S. Government.

Chairman CARPER. OK. Thank you. I have a couple of questions, a series of questions, Ms. Farrell, if I could, for you. And before I ask the questions, let me just make a short statement. But when an investigator fails to discover or disclose crucial information during a background investigation, it is an obvious failure. What could be more troubling is GAO's report that efforts by agencies to measure and improve the quality of investigations have fallen short. The Office of Personnel Management is supposed to review the investigative file and make sure it meets minimum standards. The agency responsible for granting the security clearance also has the responsibility to review the file.

Yet when GAO looked into what OPM and other Federal agencies were doing in 2008 to review the quality of background investigations, it found almost 90 percent of the investigation reports that DOD was using to evaluate an applicant for a security clearance were missing required documentation. Three questions:

First, how often were agencies making a security clearance decision without having all of the required information? And what motive did agencies have for doing this? That is the first question.

Ms. FARRELL. The answer is we do not know because GAO performed this analysis of the complete documentation for DOD in 2006 and 2009. So we do not know outside of DOD the information that you are asking for, and this is the type of oversight that we are saying is needed.

Chairman CARPER. All right. Second question: What type of information is missing? Could you give us some idea?

Mr. FARRELL. Employment verification and discussions with the employers; social references, especially the number of social references in order to determine someone's character; completeness of the application, which should be the very first step, as we have noted before, that should be done before OPM even moves forward.

Chairman CARPER. All right. Thank you. And the third question: Has GAO had an opportunity to take another look at this issue since 2008? And if you have, has there been any noted improvement?

Ms. FARRELL. We have continued to monitor OPM's actions to implement the recommendation that we made at that time. As I noted, in 2010 we were very encouraged that there was agreement among OMB, OPM, DOD, and the DNI regarding metrics for quality of investigations as well as adjudications and other aspects of the process. There was somewhat of a plan to move forward beyond

that. We have continued to monitor, but at this time all we know is that that plan has fallen apart.

Chairman CARPER. OK. Thank you.

My next question would be for Mr. Prioletti and I think for Mr. Lewis. According to some news reports, the company that hired Alexis—it is, I think, a company called "The Experts"—had phoned his hotel room in Rhode Island, I believe in August, saying that he was unstable and that the company was bringing him home.

According to other news reports, the human resources director of The Experts talked to the mother of Aaron Alexis on August 9, and she informed the company of her son's past paranoid behavior and stated that he probably needed therapy. And I would just ask, first of all, for Mr. Prioletti, if the company that had hired Alexis had become aware of the increasingly troubled behavior, do you think that the contractor should have a duty to report the behavior to the Department of Defense? And did they report it?

Mr. PRIOLETTI. Senator, in this particular case that you have just described, in terms of a national security perspective, it behooves everyone to report any unusual activity that they see, whether it be a colleague, a co-worker, or a subordinate that works for you.

Chairman CARPER. And the second half of my question was: Did they report it?

Mr. PRIOLETTI. To the best of my knowledge, sir, it was just reported to the mother, as you described there. I am not positive whether or not they reported it to DOD.

Chairman CARPER. I am going to ask both you and Mr. Lewis to answer that question for the record. I will give Mr. Lewis a chance to answer it right now.

Mr. LEWIS. The contractor is required to report any derogatory information coming to their attention regarding a cleared employee. The Defense Security Service has done a followup review at The Experts, and they have determined that the company was aware of the indications of mental instability on Mr. Alexis' part, and that they failed to report that information.

Chairman CARPER. All right. Thank you.

Mr. Lewis, stay with us in this area of questioning. What do you think should be the role of DOD contractors in monitoring the suitability of their employees to hold a clearance?

Mr. LEWIS. This is part and parcel of their responsibilities as a cleared contractor. As a prerequisite for getting a company cleared, they must execute a security agreement, and part of that security agreement is the National Industrial Security Program Operating Manual (NISPOM). They have been required to do this literally for decades. This is an established process, and contractors must execute that responsibility.

Chairman CARPER. OK. Thank you.

I would ask you to think about a question. I have given that question so you had a little time to think about it. What can we say, what can you say to those who lost their loved ones, their husbands, their wives, their moms and dads, a brother or sister, what can we say to them that might give them some comfort to know that out of the horrible tragedy in their lives, and really our country's life, what can we say today to make them feel that some good is going to come out of this? Mr. Jordan.

Mr. JORDAN. Thank you, Mr. Chairman. I would first say that we owe the survivors of this tragedy and the American people a comprehensive and thoughtful review. What information do we look at? When do we review people in the suitability and security clearance process? How are decisions made and how can we improve upon all of these aspects?

The review that I talked about will be done collaboratively. There are the Navy's reviews that have happened, Department of Defense reviews, OPM, and then the overarching review, which all of our agencies are involved in. This will not be a siloed effort. And we will act on any improvements as quickly as possible. Where there are gaps, we will close them. Where there were failures, we correct them.

But if I was one of the families of the victims, I would not just want to hear about processes and procedures. I would probably have some concerns that there is a blue-ribbon panel type creation as opposed to actual improvements, that we will do everything we can to prevent this from happening again. So I would just say to them that I live near the Navy Yard. On the morning of September 16, my wife and my 2-year-old son were actually playing in a park across the street when they were cleared by police as the tragedy was unfolding in the Navy Yard. We lost a husband of a senior member of our acquisition community.

So I would tell them that getting this right is personal to me, and we will do everything we can to improve our processes and everything under our power to make sure nothing like this happens again.

Chairman CARPER. Good. Thank you. Ms. Kaplan.

Ms. KAPLAN. Of course, I would echo what Joe said, and our hearts really were broken that day for the families and for the folks that we lost, the Federal employees and the contractors. And I think in addition to what Joe said, this is getting attention at the highest levels. The President is the one that ordered this review. And I am sure and I know that he feels very strongly in the same way that Joe just articulated that this was an awful loss, and we have to do whatever we can to prevent it from happening again.

Chairman CARPER. All right. Thank you. Mr. Prioletti.

Mr. PRIOLETTI. I also would like to echo the comments of Director Kaplan and Mr. Jordan. There are no real words to describe the loss both to this Nation as well as to family members that are sitting behind us. But I can give you a guaranteed commitment from not only the DNI but each one of us at this table that we will continue to work to find the solution. This is an evolutionary process. As we find gaps in our processes and the way we do our business, the techniques, the available information, we will continue to utilize those to come up with the best possible process to improve how we do our business on behalf of the U.S. Government as well as the U.S. citizens.

Chairman CARPER. Thank you, sir. Stephen.

Mr. LEWIS. In addition to what my fellow witnesses have had to say, I would just add that we need to make a commitment and effectively ensure that what happens between investigations is something that is tracked. We vet people. We entrust them with our classified information and access to our sensitive facilities. And we

have an obligation to ensure that we are looking at people between investigations and taking appropriate corrective action as needed.

Chairman CARPER. Thank you. Ms. Farrell.

Mr. FARRELL. I would say it is unfortunate that the tragedies that we saw at the Navy Yard focuses attention on this process. But we have seen the dedicated leadership from these executive branch agencies in the past, and when they make their minds up to take on a problem and solve it, they do it. And now is the time for actions, not just review groups.

Chairman CARPER. A lot of folks in the room know that the Government Accountability Office, is regarded as a watchdog and an arm of the legislative branch of our government to be a watchdog for really the whole expanse of the Federal Government. It is a huge job. You have a lot of people that do it, probably not enough, I am told by Gene Dodaro, the Comptroller General. But we need your continued vigilance to help us do our job, and that is the oversight role.

I think probably the two most quoted things that Ronald Reagan ever said was, one, when he said to Mr. Gorbachev, "Mr. Gorbachev, tear down this wall," as he stood at the Berlin Wall, and it was torn down. He also used to say, when he was trying to negotiate reductions in nuclear arms with the Soviet Union, he would say of his friend Gorbachev, "Trust, but verify."

All of us on the Committee, our staffs as well, trust you, and we trust the good will of the folks with whom you work who are responsible for carrying through on these reforms and to make sure it is not just words but there are actions to back it up. So we are trustful, but this Committee is going to be, in concert with GAO and you and your colleagues, we are going to be doing some verification along the way.

Ms. Kaplan, as you go off to your next assignment, we wish you well. And we again appreciate the preparation time you have given to being with us today. Even more we appreciate the commitment of those who, in your case, Ms. Kaplan, will follow you and those with whom the rest of you serve to make sure that these words are words and this promise is a promise that we keep.

With that having been said, this hearing is adjourned. Thanks so much.

[Whereupon, at 12:17 p.m., the Committee was adjourned.]

# APPENDIX

---

**Opening Statement of Chairman Thomas R. Carper**
**"The Navy Yard Tragedy: Examining Government Clearances and Background Checks"**
**October 31, 2013**

*As prepared for delivery:*

On Monday, September 16, a horrible tragedy unfolded at the Navy Yard in Washington D.C. A very troubled individual took 12 lives in a senseless act of violence. The circumstances that led to this tragedy are multi-dimensional.

Many of the issues raised by this tragedy – such as the adequacy of our gun laws and the quality of mental health care – are outside the purview of this Committee. But as we have learned more about Aaron Alexis, a number of my colleagues and I have been asking each other why such a troubled, unstable individual possessed a security clearance from the U.S. government.

Why was he originally granted a security clearance when he did not disclose his arrest record on his application? Why did the investigator responsible for looking into that arrest write up that Alexis had 'retaliated by deflating' someone's tires, instead of disclosing that Alexis had shot the tires? And we also wonder how such violence could have taken place at the Navy Yard, which is more secure than just about any workplace in the country.

The Navy Yard tragedy is not the only reason that Members of Congress are questioning the quality of the background checks. The Edward Snowden case, of course, raises many of the same questions. So have the Wikileaks disclosures by Private Bradley Manning.

Just yesterday, we learned that the Department of Justice has joined a lawsuit against a company called United States Investigations Services, commonly known as USIS. This is the company that performs about 45 percent of the background investigations that are contracted out by the Office of Personnel Management.

According to this law suit, USIS engaged in a practice that company insiders referred to as 'dumping.' Under this alleged scam, USIS would send investigations back to the Office of Personnel Management even though they had not gone through the full review process. Through this "dumping," USIS maximized its profits.

Many national security experts have long argued that the security clearance process is antiquated and in need of modernization. Given recent events, I think we have to ask whether the system is fundamentally flawed. But we should also be mindful that, for many years, both Congress and federal agencies were concerned about the backlog of security clearance applications, which grew larger after 9/11. We need to make sure that investigators do not feel pressured to sacrifice quality for speed.

Many have heard me say that almost everything I do I know I can do better. The same is true of all of us, and of most federal programs. It is in that spirit Dr. Coburn and I have convened today's hearing. Our primary purpose is to learn what we are doing right in the security clearance process while also learning how we can improve it.

We have many questions to ask. Among them are these:

- Are we looking at the right risk factors in attempting to identify people who should not be trusted with a clearance, or who could do serious harm our government and our country?

- What important information do background checks miss in the current system, which relies heavily on self-reporting by the individuals applying for a clearance?

- Once a clearance is granted, what events should trigger a re-examination of an individual's suitability to retain that clearance?

- What problems are created by the heavy reliance by the Office of Personnel Management on contractors to perform background checks?

- What are the advantages of that reliance?

- And, what is the relationship between background checks for security clearances and background checks for other types of privileges, such as access to sensitive government facilities?

We also need to ask what impacts sequestration and years of strained budgets have had on the clearance process. Under the current system, periodic re-investigations of individuals holding clearances are supposed to be done every 5 years for people with Top Secret clearances, and every 10 years for people with Secret clearances.

However, because of funding shortfalls, employees sometimes continue to work in positions that allow access to classified information, even if the initial period of clearance has lapsed. For example, this summer, for 10 weeks, the Department of Defense suspended the periodic reviews of some contractor employees due to funding shortfalls.

I would like to hear from our witnesses today about how often suspensions like that are happening across the federal government. I'd also like to hear about what agencies are doing to manage risks to our security when clearances are not re-examined on schedule through the periodic review process.

Today, we have been joined by officials from the four agencies responsible for the policies and procedures used to determine who is eligible to obtain security clearances and access to government facilities and computers. They are the Office of Management and Budget, the Office of Personnel Management, the Office of the Director of National Intelligence, and the Department of Defense.

We want these officials to talk with us this morning about these critical security-related policies and procedures, and also about the coordinated reviews of these processes now underway throughout the government in the aftermath of the Navy Yard tragedy and other recent incidents. We also will hear from an expert at the Government Accountability Office, which has produced a wide body of work on the security clearance process.

This hearing builds on the ongoing good work of our subcommittees, which held a hearing on security clearances just this past June under the leadership of Senators Tester, Portman, McCaskill and Johnson. That hearing exposed the urgent need for additional resources for the Inspector General at the Office of Personnel Management to enable that IG to conduct important oversight of background investigations.

In July, our Committee approved a portion of a bill sponsored by Senator Tester, and co-sponsored by Senators Coburn, McCaskill, Portman, Begich, Ron Johnson, Bill Nelson, and Max Baucus, to allow the Inspector General to tap into OPM's revolving fund for the purposes of performing that much-needed oversight. This legislation passed the Senate earlier this month, and I hope it will be signed into law by President Obama soon.

In closing, I want to say that the vast majority of individuals who hold security clearances are honorable and trustworthy. Many of them felt called into service after 9/11 to help protect our country. Having said that, though, we still must have a system that does a better job of rooting out those with nefarious purposes and those who become deeply troubled and unstable. That system must identify those whose behavior signals an unacceptable risk to be entrusted with classified information or access to sensitive federal facilities. I hope that our hearing today will help point us to a number of sensible solutions that – taken together – will truly improve our national security.

Finally, I think it is important to note that our Committee continues to look at other aspects of the Navy Yard tragedy, including the physical security of federal buildings, as well as preparedness, emergency response and communications issues. So, we have much work to do to learn as much as we can from this tragedy and try to prevent similar ones in the future. With that, let me welcome Dr. Coburn and say that I look forward to his opening comments.

###

----- Embargoed Until Delivery -----

**EXECUTIVE OFFICE OF THE PRESIDENT**
**OFFICE OF MANAGEMENT AND BUDGET**
**WASHINGTON, D.C. 20503**
www.whitehouse.gov/omb

**STATEMENT OF**
**THE HONORABLE JOSEPH G. JORDAN**
**ADMINISTRATOR FOR FEDERAL PROCUREMENT POLICY**
**OFFICE OF MANAGEMENT AND BUDGET**
**BEFORE THE**
**COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS**
**UNITED STATES SENATE**

**OCTOBER 31, 2013**

Chairman Carper, Ranking Member Coburn, and members of the Committee, I appreciate the opportunity to appear before you today to discuss the government's practices and procedures regarding security clearances, facility access, and suitability determinations.

As government officials, our highest duty is to protect the national security, including the confidentiality of classified information. Simultaneously, we have a separate and also critically important obligation to protect individuals performing work on behalf of Federal agencies and members of the public using Federal facilities from workplace violence. In recent years, with Congress' help, we have taken a number of important actions to strengthen both national security protections and protections relating to the physical security of Federal facilities and people who use them, such as improving the effectiveness and efficiency of background investigations and the variety of adjudications they facilitate, and strengthening the processes by which agencies make national security and suitability determinations. We must ensure those processes -- and the processes for granting and revoking access to facilities and information systems, and for conducting timely reevaluations on those persons who have been entrusted with access -- fully mitigate risks.

We have a multi-sector workforce, comprised of military, civilian, and contractor personnel. We have worked to ensure that robust vetting policies and processes are applied to all individuals with access to federal facilities, networks, or classified information in a consistent manner. This approach reflects two important principles: first, the need to protect our national security is no less critical when the work is performed by contractors than when it is performed by federal employees; second, the men and women who make up the contractor workforce are no less patriotic than their government counterparts, and in fact, many have had meaningful careers as federal employees or in the Armed Forces.

While we have made significant progress in the area of fitness and suitability, security clearance, and credentialing process reform, we need to do more. This morning, I will briefly describe several of the key reforms associated with the Administration's ongoing security clearance reform initiatives, including how these efforts are applied to work performed by contractors. I will then outline for the Committee the steps we are taking, at the President's direction, to identify and address remaining challenges.

**Background and Progress**

For far too long, the government's security clearance operations have been plagued by inefficiencies and significant expense. It has been the subject of studies and reports over the years, but little progress was made to address substantial delays, accumulating backlogs, and unnecessary costs due to workers waiting to perform the jobs for which they had already been hired. Without a "whole-of-government" approach, agencies made little progress addressing the longstanding coordination problems that compromised the timeliness and quality of the process.

Recognizing the breadth and depth of this problem, Congress took action. In 2004, Congress passed the Intelligence Reform and Terrorism Prevention Act (IRTPA), which challenged the Federal government to address these issues, and in 2005, the Government Accountability Office (GAO) placed the Department of Defense (DoD) Personnel Security Clearance Program on its high-risk list. IRTPA required all agencies to complete 90 percent of their security clearances in an average of 60 days by December 2009.

As a result of actions the Executive Branch has taken to meet the goals and objectives of IRTPA, the time to grant the average security clearance has been reduced dramatically in the past several years. In 2005, the government-wide average for initial clearances was 265 days, and, as recently as October 2006, the backlog of pending clearance investigations over 180 days old stood at almost 100,000 cases. By December 2009, compliance was achieved. That is, 90% of the government's initial clearances were completed within the IRTPA statutorily-required timeframe of 60 days. We have consistently met the IRTPA goals every quarter since, while maintaining the standards expected of the clearance process, and the decades-old backlog of initial investigations is now gone.

Importantly, Executive Branch reform efforts have also extended beyond meeting the timeliness goals established in IRTPA. In order to align suitability and national security policies and practices, and to establish enterprise information technology standards to improve efficiency and reciprocity, Executive Order 13467 established the Suitability and Security Clearance Performance Accountability Council (PAC), chaired by OMB's Deputy Director for Management, to be accountable to the President for reform goals. The Executive Order also further consolidated oversight by designating the Director of the Office of Personnel Management (OPM) and the Director of National Intelligence (DNI) as the Suitability Executive Agent and Security Executive Agent, respectively.

The PAC has worked with departments and agencies to meet a range of reform challenges. In pursuit of the goal to increase the use of information technology in making the security clearance and suitability processes more efficient, applicants are using an improved electronic questionnaire for National Security Positions, investigators have increased access to electronic record repositories, and OPM investigations are transmitted electronically. In addition, the PAC has endorsed the revised Federal Investigative Standards (FIS), which for the first time establish a fully aligned, five-tiered model for suitability and security investigations. On December 6, 2012, OMB's Deputy Director for Management directed OPM and ODNI to include in the new standards, common investigative requirements for contract employees. The implementation plan for the revised standards is nearly complete, and once fully implemented, the revised FIS will streamline and facilitate greater alignment of investigations for suitability for Federal employment, eligibility for access to classified information, eligibility to perform sensitive position duties, and fitness to work on a contract.

In response to GAO concerns that quality may suffer in the wake of focusing on timeliness, in 2008 DoD developed tools to monitor the quality of investigations and clearance adjudications. The most recent data indicate that adjudicators meet the standards for adjudication documentation, accuracy, and consistency with national standards in 99% of their cases. As a marker of the significant progress made, in 2011 GAO removed DoD's Personnel Security Clearance Program from its high-risk list. The efforts of this administration have resulted in federal hires, military personnel, cleared contractors, and those personnel requiring a reinvestigation having a more effective and expedient clearance experience than they did just a few years ago.

While significant improvements have been made, recent events clearly highlight that we need to be diligent in this effort and continue to identify and address any potential vulnerabilities in this process. These events also highlight that a weakness or gap in any part of the end-to-end process, starting from the collection of relevant information for the initial investigation to the sharing of relevant information after a favorable determination has been made, can create vulnerabilities that result in catastrophic results.

**Security and Fitness Determinations in Federal Contracting**

The government values its partnership with industry and relies on this partnership to support federal employees in meeting national security needs and to support many other vital government operations. Each year, the government spends approximately $300 billion for contracted services to support departments and agencies in carrying out their missions. In developing solicitations for these contracts, agency personnel are responsible for determining whether performance of the services will require contractor employees to have routine physical access to a federally-controlled facility, routine access to a federally-controlled information system, or access to classified materials. In cases where this access is required, contractor employees are subjected to the same general investigative requirements that are imposed on federal employees.

Both federal and contractor employees are subject to background investigations and determinations which vary in scope depending on the sensitivity and risk of the position. All Federal employees must undergo a background investigation to determine, in the first instance, whether their employment is clearly consistent with the interests of the national security. For the competitive civil service and the career Senior Executive Service, there is an additional requirement to evaluate, based on the background investigation, the person's character and conduct to decide if it may have an impact on the integrity or efficiency of federal service, which is the basis for a suitability determination. For the excepted civil service and contract employees, agencies have the option to conduct an equivalent "fitness" adjudication.

Background investigations begin with a requirement to complete the appropriate OPM standard form (SF-85, SF-85P, SF-86), depending on the sensitivity, risk, and requirement to access classified information involved in the position. Specific steps that agencies must take in connection with their federal acquisitions include the following:

- Information Collection: Contractor employees requiring access to federal facilities, federal information systems, or classified information are required to complete the same Standard Forms as federal employees, based on the sensitivity, risk, and access requirements of the position, at which point the background investigation process is initiated.
- Personal identity verification. The agency is required to incorporate a clause in the contract (i.e., FAR clause 52.204-9) which subjects contract employees to the same requirements in HSPD-12 as are imposed on federal employees. The HSPD-12 common identification standard requires personal identity verification (PIV) and background investigations for all affected contractor and subcontract personnel to support credential issuance and access to federally controlled-facilities or information systems. If a background investigation reveals derogatory information, the agency would deny issuance of the PIV card (or if such information were subsequently learned, revoke the card). Likewise, the agency can collaterally deny or revoke the card if the contract employee is subject to an unfavorable security, suitability, or fitness determination. Finally even if a contractor employee is subject to no other form of vetting, agencies can use risk-based standards issued by OPM in 2008 to deny or revoke the card.
- Contractor employee fitness. Under terms and conditions prescribed by contract, an agency may assess a contract employee's "fitness" to work on the contract, based on character and conduct. OPM has gathered and shared best practices with agency chief human capital officers to improve agencies' use of contractor fitness adjudications.
- Access to classified information. Contracting officers, pursuant to FAR 4.403(a), are required to review all proposed solicitations to determine whether access to classified information may be required by offerors, or by a contractor employee during contract performance. For contracts that involve national security interests or access to

classified information, the executive branch operates the National Industrial Security Program (or NISP), established under Executive Order 12829, to ensure these contracts are subject to national security requirements and processes equivalent to those used when the work is performed by federal employees (i.e., an agency uses the same standards and processes to determine eligibility for access to classified information irrespective of whether the individual being evaluated is employed by the government or by a government contractor). The NISP is made effective through standard contract language (i.e., FAR clause 52.204-2 or one substantially similar), which requires contractors to follow the detailed security practices outlined in the National Industrial Security Program Operating Manual (NISPOM).

Under procedures set forth in FAR Subpart 9.4, certain employees of contractors may be suspended or debarred for misconduct or other reasons that reflect adversely on the person's business honesty or integrity, or ability to perform under a Federal award. The individual's name would be posted on the System for Award Management and the individual would not be eligible to receive new federal contracts or federal financial assistance awards during the pendency of the suspension or debarment. Separately, the contractor that had employed the suspended or debarred employee may also face inquiries into their hiring and employee screening procedures. The employing contractor may also be suspended or debarred if the agency determined that the contractor is no longer presently responsible – i.e., that it lacks the business ethics and integrity to perform work for the taxpayer.

To strengthen the government's overall ability to effectively fight fraud, waste, and abuse in federal acquisition, agencies have taken a series of steps, in accordance with OMB Memorandum M-12-02, to improve their ability to consider and impose suspension and debarment to protect the government from harm. The number of suspension and debarment actions has increased as agencies have developed or reinforced programs and related internal controls to effectively use these tools to ensure the government does not do business with contractors who seek to abuse or misuse federal funds. In addition, the Federal Awardee Performance and Integrity Information System (FAPIIS), which was launched in the spring of 2010, is helping agencies root out non-responsible contractors before funds are contractually obligated by giving contracting officers one-stop access to a range of information they need to make more informed evaluations of the responsibility of prospective contractors, including contractor representations of past criminal convictions or finding of fault and liability in civil or administrative actions.

However, I would like to emphasize that formal suspension and debarment procedures are not required to remove a problematic contract employee from the federal workplace. The Federal agency may simply direct the contractor to remove the individual from the contract, or may place conditions on his or her access to the worksite.

**Moving Forward**

Once again, we recognize the serious nature of recent events and will continue to intensify our efforts to strengthen and improve our existing policies and processes. To that end, the President directed OMB to conduct a 120-day review of suitability and security processes and contractor fitness determinations. For suitability and fitness, the review will focus on whether the processes in place adequately identify applicants who, based upon their character and past conduct, may be disruptive to operations or even dangerous to the workplace. (Agencies have at their disposal a means of conducting a similar analysis for employees of contractors, by including fitness requirements in their contract provisions or by using supplementary adjudicative criteria issued by OPM at the time they make credentialing decisions for logical or physical access to Federal systems and facilities.) The focus on national security risk will center on determining eligibility and granting access that could lead to loss of classified information and damage to national security. Additionally, we will evaluate the means to collect, share, process and store information that supports these decisions, while emphasizing transactions among and equities shared across agencies.

More specifically, this review will identify and make recommendations to improve the following areas:

- Policies, processes, and procedures related to the initiation, investigation, and adjudication of background investigations for national security adjudications, suitability or fitness for employment, credentialing, and fitness to perform work on a contract.
- Accessibility of records required to meet Federal Investigative Standards such as law enforcement, health, and financial data.
- Policies, processes, procedures, and implementation efforts related to the National Industrial Security Program.

As part of these efforts, we will also be considering opportunities to improve the application of these standards and procedures to contracting, which may include, as just one example, improved information sharing between agencies suspending and debarring officials and offices responsible for making determinations for fitness and security clearances.

Our first interagency meeting is scheduled for next week and will serve to launch our review process. Additional meetings will occur over the coming weeks and we fully anticipate this review to be completed within the 120-day timeframe, which sets the release of our initial findings and recommendations for mid-February.

This review is being fully coordinated with efforts being led by the National Security Staff and OMB on the sharing and safeguarding of classified information, DoD reviews of physical and personnel security, and other ongoing related initiatives underway within the ODNI and OPM.

**Conclusion**

Once again, thank you for the opportunity to testify. As I noted in the beginning of my testimony, there is nothing more important than the two goals of protecting our people and protecting sensitive information. We have steadfastly worked in a collaborative manner to improve our processes and procedures to ensure the safety of both. As recent tragic events have highlighted however, we must maintain a strong focus on continuous improvements, and we will heed the President's call to conduct a comprehensive review and address any potential gaps in the most effective and quickest manner possible. We look forward to working with this committee and Congress as we undertake this important work.

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT

**STATEMENT OF**
**ELAINE KAPLAN**
**ACTING DIRECTOR**
**U.S. OFFICE OF PERSONNEL MANAGEMENT**

**before the**

**SENATE COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS**

**on**

**"THE NAVY YARD TRAGEDY: EXAMINING GOVERNMENT CLEARANCES AND BACKGROUND CHECKS"**

**October 31, 2013**

---

Chairman Carper, Ranking Member Coburn, and Members of the Committee, thank you for asking me to be here today. The events of September 16, 2013 were horrifying to us all, and I share your commitment to identifying and addressing the root causes for this terrible tragedy.

To that end, this Committee and others have asked the Office of Personnel Management (OPM) questions about the background investigation it conducted on Aaron Alexis in 2007 and what role that background investigation had in the Navy's decision to grant Mr. Alexis a security clearance. I appreciate the opportunity to discuss those issues with you today and to give you a better understanding of OPM's role in the security clearance process generally.

## 1. Aaron Alexis Matter

First, let me begin with Mr. Alexis' case. In 2007, at the request of the Navy, which was considering whether to grant Mr. Alexis a Secret level clearance in connection with his military service, OPM conducted a background investigation with support from a government contractor (USIS). The investigative standard for a Secret clearance in 2007 (as well as today) required a National Agency Check with Law and Credit (NACLC). The NACLC is a records based investigation – it consists of a questionnaire completed by the person being investigated and checks of Federal records, credit history records, and criminal history records. In addition to these records checks, which were completed in Mr. Alexis' case, applicable policies required a subject interview to afford Mr. Alexis the opportunity to confirm, deny, or refute the information

uncovered by the investigation that was discrepant from the personal history he provided on his security questionnaire.

It is important to understand the relatively limited nature of the investigation prescribed in the standards as they existed in 2007 for individuals like Mr. Alexis being considered for a Secret level clearance in connection with their military service. Those standards were records based, unlike the investigations for higher levels of clearance, and did not require that the investigator interview references. Each of the approximately 22,000 local law enforcement agencies in the U.S. have different policies and procedures; often their limitations are based on an inability to provide record access due to budget and staffing constraints rather than an unwillingness to comply with investigative requests. At the time of the Alexis investigation in 2007, OPM obtained the Seattle law enforcement records using the Washington Statewide database for District/Municipal Courts, as well as the King County Superior Court's database, as was standard practice at the time. The Washington courts database reported the Malicious Mischief offense, the date of offense, the dismissal of the case due to charges not being filed, and the disposition (dismissed). The database did not contain additional details regarding the offense itself.

Our quality control experts within OPM's Federal Investigative Standards division have since reviewed Mr. Alexis' file and have advised me that it complied with all applicable standards. I have also asked our office of Internal Oversight and Compliance to review the matter and make recommendations as appropriate. Finally, our Inspector General is currently examining the investigative record, and we look forward to hearing his views.

OPM's involvement with matters related to Mr. Alexis' security clearance ended when we submitted the case to the Department of Defense (DoD) for adjudication in December 2007.

## 2. The Security Clearance Program

There are a series of steps that must be taken to determine whether an individual should be granted a security clearance. The process begins when a Federal agency determines whether the duties of a particular Federal civilian position or position in the military will require the incumbent to have access to classified information, or that an employee of a contractor will require access to classified information in order to perform work under a Government contract. If such a determination is made, and if there is no prior eligibility determination that is sufficient, under applicable directives, to meet that need, the agency will need to determine such eligibility itself.

Once an agency determines that the subject will perform work that requires a demonstrated, foreseeable need for access to classified information, and that an investigation is required, the agency submits a request to OPM that it perform the background investigation. OPM performs

the investigation on a reimbursable basis in accordance with established investigative standards and then delivers the report of investigation to the requesting agency.

I want to emphasize that OPM is not charged with deciding whether an individual should or will be found eligible for access to classified information or even with making any recommendation with respect to that decision. The decision that an individual should receive access to classified information is ultimately, pursuant to Executive Order 12968, the exclusive responsibility of the head of the agency employing the individual, or his or her designee, following a national security adjudication (either by that agency or by a central adjudicative facility working on its behalf). The agency for which the work is to be performed makes the decision to grant eligibility, based, in part, upon the background investigation, and, in part upon other information that may be available to the agency, such as a polygraph if required for the position. Further, the agency can reopen the investigation or order additional investigative work from OPM if it does not have enough information to make a determination.

The security clearance process must conform with government-wide rules that include investigative standards (which may vary, based on the level of classified information to which the individual will have access), adjudicative guidelines, and reciprocity mandates. The standards outline the required elements of the investigation. These elements include the completion of a questionnaire by the applicant and specified record and other checks to be performed by OPM depending on the level of clearance sought.

Background investigations are dependent on the voluntary cooperation of sources and of records providers, as well as the availability and accessibility of references and records. In some instances, essential personnel are not available for an interview (for example, when members of the Armed Forces are deployed in dangerous locations overseas); members of the public are unwilling to provide interviews to investigators or to complete inquiry forms; or records are not made available (for example, Federal, state, and local records may not be accessible to our investigators for a variety of reasons).

Each OPM investigator who has performed work on the investigation prepares a report of investigation that details all work attempted and all work completed. These reports of investigation are combined with the results of records checks that OPM conducts of record repositories specified in the investigative standards. Further, OPM uses "issue codes" to alert the sponsoring agency of areas of potential adjudicative concern. Once the investigator completes his or her work, OPM reviews the results package for completeness (and, when efforts to complete items were unsuccessful, reporting those efforts) and delivers it to the customer agency. The delivery is generally accomplished by electronic means to support electronic adjudication processes in place at Federal agencies.

Once OPM has completed its work and transmitted the final investigation file to the customer agency, OPM's role in the investigation concludes.

### 3. Staffing and Oversight of Investigations

Adapting to change within the background investigation program is not new to the investigative community. For example, during the Clinton Administration, the decision was made to move large amounts of the background investigations work performed by OPM to a contractor workforce. The decision was made that OPM should absorb a background investigations function performed by DoD (with a Federal workforce) into the OPM workforce, leaving OPM with a blended workforce of investigators. Today, OPM continues to use a combination of Federal employees and contractors to complete background investigations. The background investigation workforce has dealt with factors that have driven down the need for background investigations – for example, declines in the size of the Federal workforce that have limited hiring, and thus the need for new background investigations to factors that have dramatically driven up the need for background investigations – for example, background investigation security needs following September 11, 2001. OPM and its partners in the background investigation community are aware of shifting demands for the investigation workforce, and working with a blend of contractors and Federal employees allows OPM to adjust its needs according to the demands of its customers.

OPM is vigilant about the potential for fraud and falsification both by Government employees and by employees of contractors. OPM has taken affirmative steps to detect and root out abuses. When instances of fraud or falsification are found, OPM takes all appropriate steps to address them. We also work closely with our Inspector General and the Department of Justice to cooperate with any subsequent investigations. We have taken steps in recent years to prevent and detect fraud and falsification both through improved workforce training and through additional levels of reviews to ensure the integrity of background security clearance investigations.

The agencies for which work is being performed control who has access to their buildings and systems, not OPM, and if an agency has concerns relating to a particular employee of a contractor, there are avenues available for that agency to take action. The agency may revoke the individual's credential and, if appropriate, direct the contractor to remove that individual from work on the contract. The agency also may request that OPM conduct a reimbursable investigation. And, of course, there are avenues for agencies to alert oversight or other law enforcement entities if there are potential criminal conduct concerns.

## 4. Steps Going Forward

During the last five years, the Office of Management and Budget (OMB), OPM, DoD, and the Office of the Director of National Intelligence (ODNI) have worked together on a reform effort to ensure that there is an efficient, aligned system for assessing suitability or fitness for Federal employment, eligibility for logical and physical access to Federal systems and facilities, eligibility for access to classified information, or fitness to perform work under a Federal contract (where required by the contract) through background investigations and appropriate adjudications. At the direction of Executive Order 13467, the Performance Accountability Council (PAC), including OPM, OMB, and ODNI, was established to ensure that the work of security clearance reform be accomplished in this context and throughout the Executive Branch.

Pursuant to Executive Order 13467, the Director of National Intelligence, as the Security Executive Agent, provides guidance and oversight of the process that government agencies use to make determinations of eligibility for access to classified information and may amend the current adjudicative criteria (established by the President) if the need arises. In addition, the Security Executive Agent is responsible for establishing the criteria governing the conduct of background investigations related to determinations of eligibility for access to classified information.

OPM, DoD, and ODNI co-chair the interagency working group chartered with establishing the first Federal standards for assessing the quality of national security and suitability background investigations government-wide. The proposed standards are currently under department and agency review with a pilot exercise to be initiated in autumn 2013 to validate ease and consistency in application of the standards.

At the President's direction, under the leadership of the Director of OMB, OPM is working with its colleagues on the PAC to review the oversight, nature and implementation of national security, credentialing, and fitness standards for individuals working at Federal facilities. Our review will focus on steps that can be taken to strengthen these processes and implementation of solutions identified during the course of recent reform efforts. In particular, we recognize that evolution of the security clearance process must include the ability to obtain and easily share relevant information on a more frequent or real-time basis.

## 5. Conclusion

The tragic events at the Navy Yard highlight the need to be ever-vigilant in ensuring that individuals entrusted with access to classified information, and, more generally, other individuals with logical and physical access to Federal facilities and information do not present either a national security risk or a personal security risk. OPM stands ready to do its part to help reduce

these risks within the scope of the matters committed to its authority, in collaboration with our colleagues on the PAC.

Thank you for this opportunity to testify, and I would be happy to answer any questions you may have.

# Statement for the Record

## Open Hearing on Security Clearance Reform

## SENATE COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

**Brian A. Prioletti**

**Assistant Director, Special Security Directorate**

**National Counterintelligence Executive**

**Office of the Director of National Intelligence**

**October 31, 2013**

Chairman Carper, Ranking Member Coburn, and distinguished Members of the Committee, thank you for the invitation to provide information on the government's practices and procedures regarding security clearances and background investigations. My statement will address the role of the Director of National Intelligence (DNI), as Security Executive Agent, his authorities and responsibilities for oversight of the security clearance process across government, areas in need of attention in the current process, and initiatives underway to address those areas.

**The DNI's Role in the Security Clearance Process**

Pursuant to Executive Order 13467, the DNI, as the Security Executive Agent, is responsible for the development and oversight of effective, efficient, uniform policies and procedures governing the timely conduct of investigations and adjudications for eligibility for access to classified information or eligibility to hold a sensitive position. The Security Executive Agent also serves as the final authority to designate agencies to conduct background investigations and determine eligibility for access to classified information, and ensures reciprocal recognition of investigations and adjudication determinations among agencies.

You requested we comment on the eligibility for logical and physical access to sensitive facilities. We defer to Director OPM, as the Suitability Executive Agent, who is responsible for developing and implementing policies and procedures relating to determinations of eligibility for logical and physical access to Federal systems and facilities.

**The Relationship Between Background Checks and the Security Clearance Process**

A background check is an essential component of the security clearance process. It is required prior to making a determination for eligibility for access to classified information or

eligibility to occupy a sensitive position. The 1997 Federal Investigative Standards, as amended in 2004, are the current standards used to conduct background investigations. The scope of the background investigation is dependent upon the level of security clearance required. A SECRET clearance includes national agency, local agency and credit checks. An interview with the individual being considered for the clearance is conducted if necessary to resolve issues resulting from the required checks. A TOP SECRET clearance requires the above checks as well as interviews of the individual being considered for the clearance, and his or her references, co-workers, supervisors, neighbors, and other individuals. Regardless of the type of clearance involved, identified issues must be fully investigated and resolved prior to any adjudication.

**The ODNI's Standards and Policies for Adjudicating Security Clearance Applications**

The Adjudicative Guidelines issued by the White House in 2005, currently serve as the government-wide guide for most eligibility decisions. The DNI has issued separate Adjudicative Guidelines for Sensitive Compartmented Information (SCI) and Special Access Program access. Adjudicative decisions are made by utilizing the whole-person concept, which is the careful weighing of available, reliable information about the person, past and present, favorable and unfavorable.

**Areas of the Security Clearance Process in Need of Attention and Potential Solutions**

Recently, two highly publicized and critical events involving individuals with clearances have further emphasized the importance of a robust security clearance program. The Committee specifically requested that we comment on the adequacy of the security clearance investigation of Aaron Alexis. A preliminary review of information made available to ODNI indicates the

work conducted during the investigation was commensurate with current investigative standards for Secret clearances.

This tragic event, as well as the Snowden incident, highlights areas in need of attention in the current security clearance process. Under the direction of the Performance Accountability Council, the ODNI, in collaboration with OMB, OPM, DoD and other federal partners, has been leading security clearance reform efforts for several years. Although these efforts are still a work in progress, when mature, they will mitigate adjudicative gaps and enhance the nation's security posture.

One critical element for a robust security clearance process is to establish an effective capability to assess an individual's continuing eligibility on a more frequent basis. Under current policies and practices, an individual's continued eligibility for access to classified information relies heavily on a periodic reinvestigation; essentially a background investigation and adjudication conducted every five years for Top Secret clearances or every ten years for Secret clearances. The time interval between periodic reinvestigations leaves the U.S. Government potentially uninformed as to behavior that poses a security or counterintelligence risk.

Continuous Evaluation (CE) is a tool that will assist in closing this information gap. Per Executive Order 13467 and the revised Federal Investigative Standards signed in 2012, CE allows for a review at any time of an individual with eligibility or access to classified information, or in a sensitive position, to ensure that the individual continues to meet the requirements for eligibility.

CE, as envisioned in the reformed security clearance process, includes automated records checks of commercial databases, government databases, and other information lawfully

available. Manual checks are inefficient and resource intensive. The CE initiative currently under development will enable us to more reliably determine an individual's eligibility to hold a security clearance or sensitive position on an ongoing basis. The DNI's CE tool must provide an enterprise-wide solution that will ensure timely sharing of relevant information across security elements of the federal government, as appropriate. A number of pilot studies have been initiated to assess the feasibility of select automated records checks and the utility of publicly available electronic information, to include social media sites, in the personnel security process. Although these pilots have identified actionable information, they indicate that retrieving, analyzing, and processing the data is likely to be resource intensive. More research is required to assess resource impacts and determine the most effective method to utilize publicly available electronic information while protecting the privacy and civil liberties of those individuals being evaluated.

In addition to supporting security clearance determinations, robust CE initiatives will also support and inform Insider Threat Programs. Damage assessments regarding individuals involved in unauthorized disclosures of classified information or acts of workplace violence have uncovered information that was not discovered during the existing security clearance process. Timely knowledge of such information might have prompted a security review or increased monitoring of the individual. We must build an enterprise-wide CE program that will promote the sharing of trustworthiness, eligibility and risk data within and across agencies to ensure that information is readily available for analysis and action.

Consistency in the quality of investigations and adjudications is another area in need of attention. The revised Federal Investigative Standards will provide clear guidance on issue

identification and resolution. They will also create an aligned system for consistent assessment of suitability, fitness, or eligibility for access to classified information for federal employment or to perform work under a federal contract. The standards will be implemented through a phased approach beginning in 2014 and continuing through 2017. In addition, the ODNI, OPM and DOD are co-chairing a working group to develop common standards and metrics for evaluating quality and comprehensiveness of background investigations. Furthermore, the ODNI has hosted a working group to refine the Adjudicative Guidelines. Recommendations regarding these guidelines are in the policy development phase.

Another initiative supporting a more robust security clearance process was the development of the National Training Standards, which were approved in August 2012 by the DNI and Director of OPM. These training standards create uniform training criteria for background investigators, national security adjudicators, and suitability adjudicators. Personnel mobility makes the application of uniform standards for conducting a background investigation and rendering an eligibility determination essential. The training standards and the revised investigative standards complement each other and when both begin implementation in 2014, will result in a more robust security clearance process that support security clearance reciprocity.

As a final note, OMB, the ODNI, and OPM are engaged in two further initiatives that will enhance security clearance processing. We are currently revising 5 Code of Federal Regulation 732, which will be reissued as 1400, to provide clarifying guidance to departments and agencies when designating national security sensitive positions. Guidance from the reissued regulation will be used to update OPM's Position Designation Tool. This will assist departments and agencies in determining position sensitivity and the type of security clearance processing

that will be required for each position. ODNI is also working with OMB and OPM to revise the Standard Form 86, *Questionnaire for National Security Positions.* This form is completed by individuals requiring security clearances and is the starting point for a background investigation. It is imperative that we collect accurate information pertinent to today's security and counterintelligence concerns.

**The DNI's Role in the President's Directive for Inter-Agency Review of the Clearance Process**

In accordance with the President's directive, OMB is conducting a review of security and suitability processes. In support of that effort, the DNI, as Security Executive Agent, will work in coordination with the OPM, DoD, and other agencies to review the policies, processes, and procedures related to the initiation, investigation, and adjudication of background investigations for personnel security, suitability for employment, and fitness to perform work on a contract.

**Closing**

Over the last five years, significant strides have been made in improving the security clearance process, particularly in the terms of timeliness and aligned national policies that provide the framework for consistency across government. I want to emphasize the DNI's resolve to lead the initiatives discussed today and to continue the collaborative efforts established with OMB, DoD, OPM and our other federal partners. I thank you for the opportunity to update the committee at this time and ODNI looks forward to working with you on these matters.

Statement of

Mr. Stephen Lewis
Deputy Director for Personnel, Industrial and Physical Security Policy
Directorate of Security Policy & Oversight
Office of Under Secretary of Defense for Intelligence

before the
Homeland Security and Government Affairs Committee
United States Senate
on

October 31, 2013

Good Afternoon

Chairman Carper, Ranking Member Coburn and distinguished Members of the Committee – I appreciate the opportunity to appear before you today to address the practices and procedures in the Department of Defense regarding security clearances, facility access, and background investigations. I am Steve Lewis, Deputy Director for Personnel Security in the Office of the Under Secretary of Defense for Intelligence, and I am here today on behalf of Under Secretary, Michael Vickers.

The Under Secretary of Defense for Intelligence (USDI) is the Principal Staff Assistant to the Secretary and Deputy Secretary for security matters. In addition, the USDI is the senior official for DoD's personnel security program and has the primary responsibility for providing and approving guidance, oversight,

and development for policy and procedures governing civilian, military, and industrial base personnel security programs within DoD.

In order to address the Department's personnel security policies and practices, I believe it is important to first identify the national level policy framework. Executive Order (E.O.) 13467 designates the Director of National Intelligence (DNI) as the Security Executive Agent with the responsibility to develop uniform policies and procedures to ensure effective completion of investigations and determinations of eligibility, for access to classified information or to hold National Security Positions, as well as reciprocal acceptance of those determinations. In addition, E.O. 13467 designates the Director of the Office of Personnel Management (OPM), as the Suitability Executive Agent, with responsibility for developing and implementing uniform and consistent policies and procedures regarding investigations and adjudications, relating to determinations of suitability and eligibility for logical and physical access to Federal Government installations and information systems. Finally, E.O. 13467 creates a Performance Accountability Council, chaired by the Deputy Director for Management, Office of Management and Budget, and including the DNI and the Director OPM, with the responsibility to ensure alignment of suitability, security, and, as appropriate, contractor employee fitness investigative and adjudicative processes.

With regard to the oversight roles and responsibilities within the DoD, the heads of DoD Components are responsible for establishing and overseeing implementation of procedures to ensure prompt reporting of significant derogatory information, unfavorable administrative actions, and adverse actions related to its personnel, to appropriate officials within their component and, as applicable, to the DoD Consolidated Adjudication Facility. This responsibility applies to military service members, DoD civilians, and embedded contractor personnel.

Under the National Industrial Security Program (NISP), cleared contractors are required to report adverse information coming to their attention regarding their cleared employees. In addition, the Defense Security Service (DSS) is responsible for conducting oversight of companies cleared to perform on classified contracts for DoD and 26 other federal departments and agencies that use DoD industrial security services.

The Department has worked very hard to create improvements that produced greater efficiencies and effectiveness in the phases of initiating and adjudicating background investigations. As a result, in 2011, the Government Accountability Office removed the DoD's personnel security clearance program from the high risk list.

We have used multiple initiatives to review and confirm (1) the quality of the investigative products we receive, (2) the quality of our adjudications, and (3)

the accuracy and completeness of the documentation of adjudicative rationale in support of appropriate oversight and reciprocity. In addition, we have implemented a certification process for DoD personnel security adjudicators.

In May, 2012, the Deputy Secretary of Defense directed the consolidation of all adjudicative functions and resources (except for DoD Intelligence Agencies) at Fort Meade, Maryland, under the direction, command, and control of the Director of Administration and Management (DA&M). This decision was made in order to maximize the efficiencies realized by the collocation of the various Centralized Adjudications Facilities (CAFs) under the 2005 round of Base Realignment and Closure (BRAC). Effective October 1st, the DoD CAF has also been tasked to adjudicate background investigations which serve as the basis for the issuance of Common Access Cards (CACs) used for physical access to DoD installations and access to DoD information systems.

I thank you for your time, and look forward to answering your questions.

United States Government Accountability Office

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

For Release on Delivery
Expected at 10:00 a.m. EDT
Thursday, October 31, 2013

# PERSONNEL SECURITY CLEARANCES

## Full Development and Implementation of Metrics Needed to Measure Quality of Process

Statement of Brenda S. Farrell, Director
Defense Capabilities and Management

GAO-14-157T

# GAO Highlights

Highlights of GAO-14-157T, a testimony before the Committee on Homeland Security and Governmental Affairs, U.S. Senate

## Why GAO Did This Study

A high-quality personnel security clearance process is necessary to minimize the associated risks of unauthorized disclosures of classified information and to help ensure that information about individuals with criminal activity or other questionable behavior is identified and considered as part of the process for granting or retaining clearances. Personnel security clearances offer individuals access to classified information that, through unauthorized disclosure, can in some cases cause exceptionally grave damage to U.S. national security. In 2012, the DNI reported that more than 4.8 million federal government and contractor employees held or were eligible to hold a security clearance. GAO has reported that the federal government spent over $1 billion to conduct background investigations in support of security clearances and suitability determinations—the consideration of character and conduct for federal employment in fiscal year 2011.

This testimony addresses the (1) extent to which executive branch agencies have metrics to help determine the quality of the security clearance process, and (2) extent that executive branch agencies have metrics to help determine the quality of the suitability clearance process. This testimony is based on GAO work issued between 2008 and 2013 on DOD's personnel security clearance program and government-wide quality and security clearance reform efforts. As part of that work, GAO (1) reviewed relevant federal guidance and processes, (2) submitted agency data on the timeliness and quality of clearance and adjudication, (3) assessed reform efforts, and (4) reviewed samples of case files for DOD personnel.

View GAO-14-157T. For more information, contact Brenda S. Farrell at (202) 512-3604 or farrellb@gao.gov.

October 31, 2013

# PERSONNEL SECURITY CLEARANCES

## Full Development and Implementation of Metrics Needed to Measure Quality of Process

### What GAO Found

Multiple executive branch agencies are responsible for different steps of the multi-phased personnel security clearance process that includes: determination of whether a position requires a clearance, application submission, investigation, and adjudication. Agency officials must first determine whether a federal civilian position requires access to classified information. The Director of National Intelligence (DNI) and the Office of Personnel Management (OPM) are in the process of issuing a joint revision to the regulations guiding this step in response to GAO's 2012 recommendation that the DNI issue policy and guidance for the determination, review, and validation of requirements. After an individual has been selected for a federal civilian position that requires a personnel security clearance and the individual submits an application for a clearance, investigators—often contractors—from OPM conduct background investigations for most executive branch agencies. Adjudicators from requesting agencies use the information from these investigations and consider federal adjudicative guidelines to determine whether an applicant is eligible for a clearance. Further, individuals are subject to reinvestigations at intervals that are dependent on the level of security clearance. For example, top secret and secret clearance holders are to be reinvestigated every 5 years and 10 years, respectively.

Executive branch agencies have not fully developed and implemented metrics to measure quality throughout the personnel security clearance process. For more than a decade, GAO has emphasized the need to build and monitor quality throughout the personnel security clearance process to promote oversight and positive outcomes such as maximizing the likelihood that individuals who are security risks will be scrutinized more closely. For example, GAO reported in May 2009 that, with respect to initial top secret clearances adjudicated in July 2008 for the Department of Defense (DOD), documentation was incomplete for most of OPM's investigative reports. GAO independently estimated that 87 percent of about 3,500 investigative reports that DOD adjudicators used to make clearance eligibility decisions were missing some required documentation, such as the verification of all of the applicant's employment. GAO also estimated that 12 percent of the 3,500 reports did not contain the required personal subject interview. In 2009, GAO recommended that OPM measure the frequency with which its investigative reports met federal investigative standards in order to improve the quality of investigation documentation. As of August 2013, however, OPM had not implemented this recommendation. GAO's 2009 report also identified issues with the quality of DOD adjudications. Specifically, GAO estimated that 22 percent of about 3,500 initial top secret clearances that were adjudicated favorably did not contain all the required documentation. As a result, in 2009 GAO recommended that DOD measure the frequency with which adjudicative files meet requirements. In November 2009, DOD issued a memorandum that established a tool called the Review of Adjudication Documentation Accuracy and Rationales (RADAR) to measure the frequency with which adjudicative files meet the requirements of DOD regulation. According to a DOD official, RADAR had been used in fiscal year 2010 to evaluate some adjudications, but was not used in fiscal year 2011 due to funding shortfalls. DOD restarted the use of RADAR in fiscal year 2012.

Chairman Carper, Ranking Member Coburn, and Members of the Committee:

Thank you for the opportunity to be here to participate in this discussion of the federal government's process for personnel security clearances. A high-quality personnel security clearance process is necessary to minimize the associated risks of unauthorized disclosures of classified information and to help ensure that information about individuals with criminal activity or other questionable behavior is identified and assessed as part of the process for granting or retaining clearances. However, recent events, such as unauthorized disclosures of classified information, have shown that there is more work to be done by federal agencies to help ensure the process functions effectively and efficiently, so that only trustworthy individuals obtain and keep security clearances and the resulting access to classified information that clearances make possible.

As you know, we have an extensive body of work on issues related to the personnel security clearance process going back over a decade. Since 2008, we have focused on the government-wide effort to reform the security clearance process. Personnel security clearances allow government and industry personnel (contractors) to gain access to classified information that, through unauthorized disclosure, can in some cases cause exceptionally grave damage to U.S. national security. It is important to keep in mind that security clearances allow for access to classified information on a need to know basis. Federal agencies also use other processes and procedures to determine if an individual should be granted access to certain government buildings or facilities or be employed as either a military, federal civilian employee, or contractor for the federal government. Separate from, but related to, personnel security clearances are determinations of suitability that the executive branch uses to ensure individuals are suitable, based on character and conduct, for federal employment in their agency or position.

The federal government processes a high volume of personnel security clearances at significant costs. In 2012, the Director of National Intelligence (DNI) reported that more than 4.9 million federal government and contractor employees held or were eligible to hold a security clearance, which poses a formidable challenge to those responsible for deciding who should be granted a clearance. Furthermore, the federal government spent over $1 billion to conduct more than 2 million background investigations (in support of both personnel security clearances and suitability determinations for government employment outside of the intelligence community) in fiscal year 2011. The

Department of Defense (DOD) accounts for the majority of all personnel security clearances—which includes 788,000 background investigations that cost over $787 million in fiscal year 2011.[1]

My testimony today will focus on two topics related to personnel security clearances. First, I will discuss the overall personnel security clearance process, including roles and responsibilities for investigations and adjudications. Second, I will discuss the extent that executive branch agencies have developed and implemented metrics to help determine the quality of the security clearance process.

My testimony is based on our reports and testimonies issued from 2008 through 2013 on DOD's personnel security clearance program and government-wide suitability and security clearance reform efforts. A list of these related products appears at the end of my statement. As part of the work for these products, we reviewed statutes, federal guidance and processes, examined agency data on the timeliness and quality of investigations and adjudications, assessed reform efforts, and reviewed a sample of investigative and adjudication files for DOD personnel. The work upon which this testimony is based was conducted in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. Further details about the scope and methodology can be found in each of these related products.

## The Overall Personnel Security Clearance Process

Multiple executive-branch agencies have key roles and responsibilities for different steps of the federal government's personnel security clearance process. For example, in 2008, Executive Order 13467[2] designated the DNI as the Security Executive Agent. As such, the DNI is responsible for developing policies and procedures to help ensure the effective, efficient,

[1]GAO, *Background Investigations: Office of Personnel Management Needs to Improve Transparency of Its Pricing and Seek Cost Savings*, GAO-12-197 (Washington, D.C.: Feb. 28, 2012).

[2]Executive Order No. 13467, *Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information* (June 30, 2008).

and timely completion of background investigations and adjudications relating to determinations of eligibility for access to classified information and eligibility to hold a sensitive position. In turn, executive branch agencies determine which of their positions—military, civilian, or private-industry contractors—require access to classified information and, therefore, which people must apply for and undergo a personnel security clearance investigation. Investigators—often contractors—from Federal Investigative Services within the Office of Personnel Management (OPM)[3] conduct these investigations for most of the federal government using federal investigative standards and OPM internal guidance as criteria for collecting background information on applicants.[4] OPM provides the resulting investigative reports to the requesting agencies for their internal adjudicators, who use the information along with the federal adjudicative guidelines to determine whether an applicant is eligible for a personnel security clearance. DOD is OPM's largest customer, and its Under Secretary of Defense for Intelligence (USD(I)) is responsible for developing, coordinating, and overseeing the implementation of DOD policy, programs, and guidance for personnel, physical, industrial, information, operations, chemical/biological, and DOD Special Access Program security. Additionally, the Defense Security Service, under the authority, direction, and control of USD(I), manages and administers the

[3]OPM's Federal Investigative Services employs both federal and contract investigators to conduct work required to complete background investigations. The federal staff constitutes about 25 percent of that workforce, while OPM currently also has contracts for investigative fieldwork with several investigation firms, constituting the remaining 75 percent of its investigative workforce.

[4]In 2005, the Office of Management and Budget designated OPM as the agency responsible for, among other things, the day-to-day supervision and monitoring of security clearance investigations, and for tracking the results of individual agency-performed adjudications, subject to certain exceptions. However, the Office of the Director of National Intelligence can designate other agencies as an "authorized investigative agency" pursuant to 50 U.S.C. § 3341(b)(3), as implemented through Executive Order 13467. Alternatively, under 5 U.S.C. § 1104(a)(2), OPM can redelegate any of its investigative functions subject to performance standards and a system of oversight prescribed by OPM under 5 U.S.C. § 1104(b). Agencies without delegated authority rely on OPM to conduct their background investigations while agencies with delegated authority—including the Defense Intelligence Agency, National Security Agency, National Geospatial-Intelligence Agency, Central Intelligence Agency, Federal Bureau of Investigation, National Reconnaissance Office, and Department of State—have been authorized to conduct their own background investigations.

DOD portion of the National Industrial Security Program[5] for the DOD components and other federal agencies by agreement, as well as providing security education and training, among other things.

Section 3001 of the Intelligence Reform and Terrorism Prevention Act of 2004[6] prompted government-wide suitability and security clearance reform. The act required, among other matters, an annual report to Congress—in February of each year from 2006 through 2011—about progress and key measurements on the timeliness of granting security clearances. It specifically required those reports to include the periods of time required for conducting investigations and adjudicating or granting clearances. However, the Intelligence Reform and Terrorism Prevention Act requirement for the executive branch to annually report on its timeliness expired in 2011. More recently the Intelligence Authorization Act of 2010[7] established a new requirement that the President annually report to Congress the total amount of time required to process certain security clearance determinations for the previous fiscal year for each element of the Intelligence Community.[8] The Intelligence Authorization Act of 2010 additionally requires that those annual reports include the total number of active security clearances throughout the United States government, to include both government employees and contractors. Unlike the Intelligence Reform and Terrorism Prevention Act of 2004 reporting requirement, the requirement to submit these annual reports does not expire.

In 2007, DOD and the Office of the Director of National Intelligence (ODNI) formed the Joint Security Clearance Process Reform Team, known as the Joint Reform Team, to improve the security clearance process government-wide. In a 2008 memorandum, the President called for a reform of the security clearance and suitability determination

[5]The National Industrial Security Program was established by Executive Order 12829 to safeguard Federal Government classified information that is released to contractors, licensees, and grantees of the United States Government. Executive Order 12829, *National Industrial Security Program* (Jan. 6, 1993, as amended).

[6]Pub. L. No. 108-458 (2004) (relevant sections codified at 50 U.S.C. § 3341).

[7]Pub. L. No. 111-259, § 367 (2010) (codified at 50 U.S.C. § 3104).

[8]This timeliness reporting requirement applies only to the elements of the Intelligence Community; it does not cover non-intelligence agencies that were covered by the reporting requirements in the Intelligence Reform and Terrorism Prevention Act of 2004.

processes and subsequently issued Executive Order 13467,[9] which in addition to designating the DNI as the Security Executive Agent, also designated the Director of OPM as the Suitability Executive Agent. Specifically, the Director of OPM, as Suitability Executive Agent, is responsible for developing policies and procedures to help ensure the effective, efficient, and timely completion of investigations and adjudications relating to determinations of suitability, to include consideration of an individual's character or conduct. Further, the executive order established a Suitability and Security Clearance Performance Accountability Council to oversee agency progress in implementing the reform vision. Under the executive order, this council is accountable to the President for driving implementation of the reform effort, including ensuring the alignment of security and suitability processes, holding agencies accountable for implementation, and establishing goals and metrics for progress. The order also appointed the Deputy Director for Management at the Office of Management and Budget as the chair of the council.[10]

## Steps in the Personnel Security Clearance Process

In the first step of the personnel security clearance process, executive branch officials determine the requirements of a federal civilian position, including assessing the risk and sensitivity level associated with that position, to determine whether it requires access to classified information and, if required, the level of access. Security clearances are generally categorized into three levels: top secret, secret, and confidential.[11] The level of classification denotes the degree of protection required for information and the amount of damage that unauthorized disclosure could

[9]Executive Order No. 13467, *Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information* (June 30, 2008).

[10]The Performance Accountability Council is comprised of the Director of National Intelligence as the Security Executive Agent, the Director of OPM as the Suitability Executive Agent, and the Deputy Director for Management, Office of Management and Budget, as the chair with the authority to designate officials from additional agencies to serve as members. As of June 2012, the council included representatives from the Departments of Defense, Energy, Health and Human Services, Homeland Security, State, Treasury, and Veterans Affairs, and the Federal Bureau of Investigation.

[11]A top secret clearance is generally also required for access to Sensitive Compartmented Information—classified intelligence information concerning or derived from intelligence sources, methods, or analytical processes that is required to be protected within formal access control systems established and overseen by the Director of National Intelligence.

reasonably be expected to cause to national defense or foreign relations. A sound requirements process is important because requests for clearances for positions that do not need a clearance or need a lower level of clearance increase investigative workloads and costs. In 2012, we reported that the DNI, as the Security Executive Agent, had not provided agencies clearly defined policy and procedures to consistently determine if a position requires a security clearance, or established guidance to require agencies to review and revise or validate existing federal civilian position designations.[12] We recommended that the DNI issue policy and guidance for the determination, review, and validation of requirements, and ODNI concurred with those recommendations, stating that it recognized the need to issue or clarify policy. Currently, OPM and ODNI are in the process of issuing a joint revision to the regulations guiding requirements determination. Specifically, according to officials from the ODNI, these offices had obtained permission from the President to re-issue the federal regulation jointly, drafted the proposed rule, and obtained public input on the regulation by publishing it in the Federal Register. According to ODNI and OPM officials, they will jointly review and address comments and prepare the final rule for approval from the Office of Management and Budget.

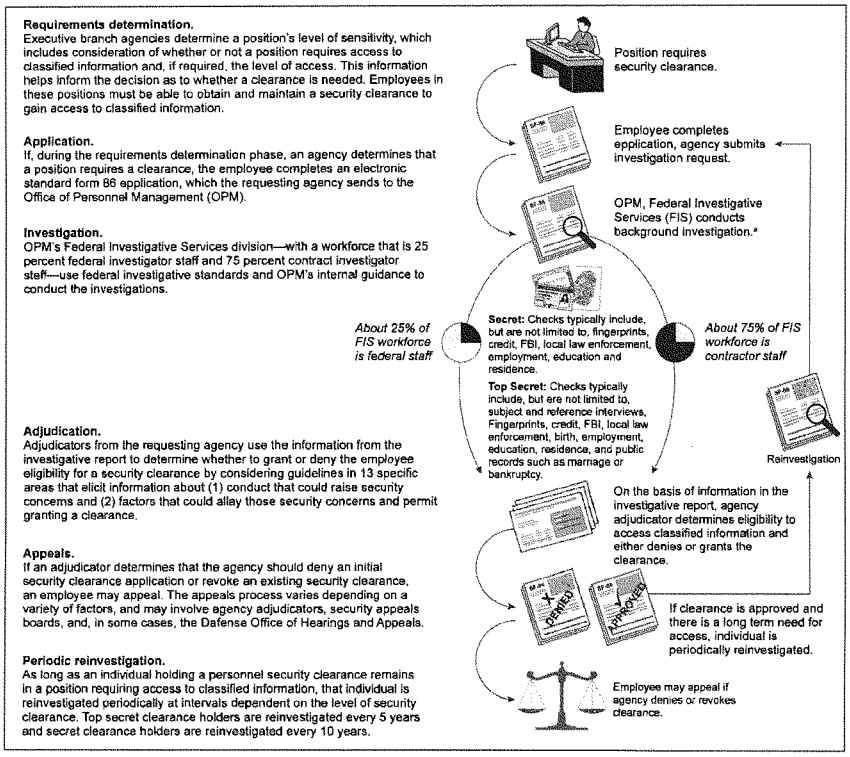
Once an applicant is selected for a position that requires a personnel security clearance, the applicant must obtain a security clearance in order to gain access to classified information. While different departments and agencies may have slightly different personnel security clearance processes, the phases that follow—application submission, investigation, and adjudication—are illustrative of a typical process.[13] Since 1997, federal agencies have followed a common set of personnel security investigative standards and adjudicative guidelines for determining whether federal civilian workers, military personnel, and others, such as private industry personnel contracted by the government, are eligible to hold a security clearance. Figure 1 illustrates the steps in the personnel security clearance process, which is representative of the general

[12]GAO, *Security Clearances: Agencies Need Clearly Defined Policy for Determining Civilian Position Requirements*, GAO-12-800 (Washington, D.C.: July 12, 2012).

[13]The general process for performing a background investigation for either a secret or top secret clearance is the same; however, the level of detail and types of information gathered for a top secret clearance is more substantial than a secret clearance.

process followed by most executive branch agencies and includes procedures for appeals and renewals.

**Figure 1: Steps in the Personnel Security Clearance Process**




Source: GAO analysis.

[a]OPM provides background investigation services to over 100 executive branch agencies; however, others, including some agencies in the Intelligence Community, have been delegated authority from the Office of the Director of National Intelligence, OPM, or both, to conduct their own background investigations.

During the application submission phase, a security officer from an executive branch agency (1) requests an investigation of an individual requiring a clearance; (2) forwards a personnel security questionnaire (Standard Form 86) using OPM's electronic Questionnaires for Investigations Processing (e-QIP) system or a paper copy of the Standard Form 86 to the individual to complete; (3) reviews the completed questionnaire; and (4) sends the questionnaire and supporting documentation, such as fingerprints and signed waivers, to OPM or its investigation service provider.

During the investigation phase, investigators—often contractors—from OPM's Federal Investigative Services use federal investigative standards and OPM's internal guidance to conduct and document the investigation of the applicant. The scope of information gathered in an investigation depends on the needs of the client agency and the personnel security clearance requirements of an applicant's position, as well as whether the investigation is for an initial clearance or a reinvestigation to renew a clearance. For example, in an investigation for a top secret clearance, investigators gather additional information through more time-consuming efforts, such as traveling to conduct in-person interviews to corroborate information about an applicant's employment and education. However, many background investigation types have similar components. For instance, for all investigations, information that applicants provide on electronic applications are checked against numerous databases. Both secret and top secret investigations contain credit and criminal history checks, while top secret investigations also contain citizenship, public record, and spouse checks as well as reference interviews and an Enhanced Subject Interview to gain insight into an applicant's character. Table 1 highlights the investigative components generally associated with the secret and top secret clearance levels. After OPM, or the designated provider, completes the background investigation, the resulting investigative report is provided to the adjudicating agency.

**Table 1: Information Gathered in Conducting a Typical Investigation to Determine Suitability and Eligibility for a Personnel Security Clearance**

| Type of information gathered by component | Type of background investigation | |
|---|---|---|
| | Secret | Top Secret |
| 1. Personnel security questionnaire: The reported answers on an electronic SF-85P or SF-86 form | X | X |
| 2. Fingerprints: Fingerprints submitted electronically or manually | X | X |
| 3. National agency check: Data from Federal Bureau of Investigation, military records, and other agencies as required (with fingerprint) | X | X |
| 4. Credit check: Data from credit bureaus where the subject lived/worked/attended school for at least 6 months | X | X |
| 5. Local agency checks: Data from law enforcement agencies where the subject lived/worked/attended school during the past 10 years or—in the case of reinvestigations—since the last security clearance investigation | X | X |
| 6. Date and place of birth: Corroboration of information supplied on the personnel security questionnaire | | X |
| 7. Citizenship: For individuals born outside of the United States, verification of U.S. citizenship directly from the appropriate registration authority | | X |
| 8. Education: Verification of most recent or significant claimed attendance, degree, or diploma | V | X |
| 9. Employment: Review of employment records and interviews with workplace references, such as supervisors and coworkers | V | X |
| 10. References: Data from interviews with subject-identified and investigator-developed leads | V | X |
| 11. National agency check for spouse or cohabitant: Data from Federal Bureau of Investigation, military records, and other agencies as required (without fingerprint) | | X |
| 12. Former spouse: Data from interview(s) conducted with spouse(s) divorced within the last 10 years or since the last investigation or reinvestigation | | X |
| 13. Neighborhoods: Interviews with neighbors and verification of residence through records check | V | X |
| 14. Public records: Verification of issues, such as bankruptcy, divorce, and criminal and civil court cases | | X |
| 15. Enhanced Subject Interview: Collection of relevant data, resolution of significant issues or inconsistencies | a | X |

Source: DOD and OPM

Note: The content and amount of information collected as part of a personnel security clearance investigation is dependent on a variety of case-specific factors, including the history of the applicant and the nature of the position; however, items 1-15 are typically collected for the types of investigations indicated.

V = Components with this notation are checked through a mail voucher sent by OPM's Federal Investigative Services.

[a]The Enhanced Subject Interview was developed by the Joint Reform Team and implemented by OPM in 2011 and serves as an in-depth discussion between the interviewer and the subject to ensure a full understanding of the applicant's information, potential issues, and mitigating factors. It is included in a Minimum Background Investigation, one type of suitability investigation, and can be triggered by the presence of issues in a secret level investigation.

During the adjudication phase, adjudicators from the hiring agency[14] use the information from the investigative report to determine whether an applicant is eligible for a security clearance. To make clearance eligibility decisions, the adjudication guidelines specify that adjudicators consider 13 specific areas that elicit information about (1) conduct that could raise security concerns and (2) factors that could allay those security concerns and permit granting a clearance.[15] If a clearance is denied or revoked, appeals of the adjudication decision are possible. We have work underway to review the process for security revocations. We expect to issue a report on this process by spring of 2014.

Once an individual has obtained a personnel security clearance and as long as they remain in a position that requires access to classified national security information, that individual is reinvestigated periodically at intervals that are dependent on the level of security clearance. For example, top secret clearance holders are reinvestigated every 5 years, and secret clearance holders are reinvestigated every 10 years. Some of the information gathered during a reinvestigation would focus specifically

[14]For industry personnel, the Defense Security Service (DSS) adjudicated clearance eligibility for DOD and 24 other federal agencies, by agreement, using OPM-provided investigative reports. However, DOD is in the process of consolidating its adjudication facilities, including those for industry personnel. Per DOD 5220.22-M, *National Industrial Security Program: Operating Manual* (Feb. 28, 2006 incorporating changes Mar. 28, 2013), those agencies are: (1) National Aeronautics and Space Administration; (2) Department of Commerce; (3) General Services Administration; (4) Department of State; (5) Small Business Administration; (6) National Science Foundation; (7) Department of the Treasury; (8) Department of Transportation; (9) Department of the Interior; (10) Department of Agriculture; (11) Department of Labor; (12) Environmental Protection Agency; (13) Department of Justice; (14) Federal Reserve System; (15) Government Accountability Office; (16) U.S. Trade Representative; (17) U.S. International Trade Commission; (18) U.S. Agency for International Development; (19) Nuclear Regulatory Commission; (20) Department of Education; (21) Department of Health and Human Services; (22) Department of Homeland Security; (23) Federal Communications Commission; and (24) Office of Personnel Management.

[15]Federal guidelines state that clearance decisions require a common sense determination of eligibility for access to classified information based upon careful consideration of the following 13 areas: allegiance to the United States; foreign influence; foreign preference; sexual behavior; personal conduct; financial considerations; alcohol consumption; drug involvement; emotional, mental, and personality disorders; criminal conduct; security violations; outside activities; and misuse of information technology systems. Further, the guidelines require adjudicators to evaluate the relevance of an individual's overall conduct by considering factors such as the nature, extent, and seriousness of the conduct; the circumstances surrounding the conduct, to include knowledgeable participation; the frequency and recency of the conduct; and the individual's age and maturity at the time of the conduct, among others.

on the period of time since the last approved clearance, such as a check of local law enforcement agencies where an individual lived and worked since the last investigation. Further, the Joint Reform Team began an effort to review the possibility of continuous evaluations, which would ascertain on a more frequent basis whether an eligible employee with access to classified information continues to meet the requirements for access. Specifically, the team proposed to move from periodic review to that of continuous evaluation, meaning annually for top secret and similar positions and at least once every five years for secret or similar positions, as a means to reveal security-relevant information earlier than the previous method, and provide increased scrutiny on populations that could potentially represent risk to the government because they already have access to classified information. The current federal investigative standards state that the top secret level of security clearances may be subject to continuous evaluation.

## Full Development and Implementation of Metrics Needed to Determine Quality of Personnel Security Clearance Process

The executive branch has developed some metrics to assess quality at different phases of the personnel security clearance process; however, those metrics have not been fully developed and implemented. To promote oversight and positive outcomes, such as maximizing the likelihood that individuals who are security risks will be scrutinized more closely, we have emphasized, since the late 1990s,[16] the need to build and monitor quality throughout the personnel security clearance process. Having assessment tools and performance metrics in place is a critical initial step toward instituting a program to monitor and independently validate the effectiveness and sustainability of corrective measures. However, we have previously reported that executive branch agencies have not fully developed and implemented metrics to measure quality in key aspects of the personnel security clearance process, including: (1) investigative reports; (2) adjudicative files; and (3) the reciprocity of personnel security clearances, which is an agency's acceptance of a background investigation or clearance determination completed by any authorized investigative or adjudicative executive branch agency.

[16]GAO, *DOD Personnel: Inadequate Personnel Security Investigations Pose National Security Risks*, GAO/NSIAD-00-12 (Washington, D.C.: Oct. 27, 1999).

## Metrics Not Yet Implemented to Measure Completeness of OPM Investigative Reports

We have previously identified deficiencies in OPM's investigative reports—results from background investigations—but as of August 2013 OPM had not yet implemented metrics to measure the completeness of these reports. OPM supplies about 90 percent of all federal clearance investigations, including those for DOD. For example, in May 2009 we reported that, with respect to DOD initial top secret clearances adjudicated in July 2008, documentation was incomplete for most OPM investigative reports. We independently estimated that 87 percent of about 3,500 investigative reports that DOD adjudicators used to make clearance decisions were missing at least one type of documentation required by federal investigative standards. The type of documentation most often missing from investigative reports was verification of all of the applicant's employment, followed by information from the required number of social references for the applicant and complete security forms. We also estimated that 12 percent of the 3,500 investigative reports did not contain a required personal subject interview.

At the time of our 2009 review, OPM did not measure the completeness of its investigative reports, which limited the agency's ability to explain the extent or the reasons why some reports were incomplete. As a result of the incompleteness of OPM's investigative reports on DOD personnel, we recommended in May 2009 that OPM measure the frequency with which its investigative reports meet federal investigative standards, so that the executive branch can identify the factors leading to incomplete reports and take corrective actions.[17]

In a subsequent February 2011 report, we noted that OMB, ODNI, DOD, and OPM leaders had provided congressional members with metrics to assess the quality of the security clearance process, including investigative reports and other aspects of the process.[18] For example, the Rapid Assessment of Incomplete Security Evaluations was one tool the executive branch agencies planned to use for measuring quality, or

[17]GAO, *DOD Personnel Clearances: Comprehensive Timeliness Reporting, Complete Clearance Documentation, and Quality Measures Are Needed to Further Improve the Clearance Process*, GAO-09-400 (Washington, D.C.: May 19, 2009).

[18]GAO, *High-Risk Series: An Update*, GAO-11-278 (Washington, D.C.: Feb. 2011).

completeness, of OPM's background investigations.[19] However, according to an OPM official in June 2012, OPM chose not to use this tool. Instead, OPM opted to develop another tool. In following up on our 2009 recommendations, as of August 2013, OPM had not provided enough details on its tool for us to determine if the tool had met the intent of our 2009 recommendation, and included the attributes of successful performance measures identified in best practices, nor could we determine the extent to which the tool was being used.

OPM also assesses the quality of investigations based on voluntary reporting from customer agencies. Specifically, OPM tracks investigations that are (1) returned for rework from the requesting agency, (2) identified as deficient using a web-based customer satisfaction survey, or (3) identified as deficient through adjudicator calls to OPM's quality hotline. However, in our past work, we have noted that the number of investigations returned for rework is not by itself a valid indicator of the quality of investigative work because DOD adjudication officials told us that they have been reluctant to return incomplete investigations in anticipation of delays that would impact timeliness. Further, relying on agencies to voluntarily provide information on investigation quality may not reflect the quality of OPM's total investigation workload. We are beginning work to further review OPM's actions to improve the quality of investigations.

We have also reported that deficiencies in investigative reports affect the quality of the adjudicative process. Specifically, in November 2010, we reported that agency officials who utilize OPM as their investigative service provider cited challenges related to deficient investigative reports as a factor that slows agencies' abilities to make adjudicative decisions. The quality and completeness of investigative reports directly affects adjudicator workloads, including whether additional steps are required before adjudications can be made, as well as agency costs. For example, some agency officials noted that OPM investigative reports do not include complete copies of associated police reports and criminal record checks. Several agency officials stated that in order to avoid further costs or delays that would result from working with OPM, they often choose to

[19]The Rapid Assessment of Incomplete Security Evaluations tool was developed by DOD to track the quality of investigations conducted by OPM for DOD personnel security clearance investigations, measured as a percent of investigations completed that contained deficiencies.

perform additional steps internally to obtain missing information. According to ODNI and OPM officials, OPM investigators provide a summary of police and criminal reports and assert that there is no policy requiring inclusion of copies of the original records. However, ODNI officials also stated that adjudicators may want or need entire records as critical elements may be left out. For example, according to Defense Office of Hearings and Appeals officials, in one case, an investigator's summary of a police report incorrectly identified the subject as a thief when the subject was actually the victim.

## DOD Has Taken Steps to Implement Measures to Determine Completeness of Adjudicative Files

DOD has taken some intermittent steps to implement measures to determine the completeness of adjudicative files to address issues identified in our 2009 report regarding the quality of DOD adjudications. In 2009, we found that some clearances were granted by DOD adjudicators even though some required data were missing from the OPM investigative reports used to make such determinations. For example, we estimated in our 2009 review that 22 percent of the adjudicative files for about 3,500 initial top secret clearances that were adjudicated favorably did not contain all the required documentation, even though DOD regulations require that adjudicators maintain a record of each favorable and unfavorable adjudication decision and document the rationale for granting clearance eligibility to applicants with security concerns revealed during the investigation.[20] Documentation most frequently missing from adjudicative files was the rationale for granting security clearances to applicants with security concerns related to foreign influence, financial considerations, and criminal conduct. At the time of our 2009 review, DOD did not measure the completeness of its adjudicative files, which limited the agency's ability to explain the extent or the reasons why some files are incomplete.

In 2009, we made two recommendations to improve the quality of adjudicative files. First, we recommended that DOD measure the frequency with which adjudicative files meet requirements, so that the executive branch can identify the factors leading to incomplete files and include the results of such measurement in annual reports to Congress

[20]DOD Regulation 5200.2-R, *DOD Personnel Security Program* (Jan. 1987, incorporating changes Feb. 23, 1996).

on clearances.[21] In November 2009, DOD subsequently issued a memorandum that established a tool to measure the frequency with which adjudicative files meet the requirements of DOD regulation. Specifically, the DOD memorandum stated that it would use a tool called the Review of Adjudication Documentation Accuracy and Rationales, or RADAR, to gather specific information about adjudication processes at the adjudication facilities and assess the quality of adjudicative documentation. In following up on our 2009 recommendations, as of 2012, a DOD official stated that RADAR had been used in fiscal year 2010 to evaluate some adjudications, but was not used in fiscal year 2011 due to funding shortfalls. DOD restarted the use of RADAR in fiscal year 2012.

Second, we recommended that DOD issue guidance to clarify when adjudicators may use incomplete investigative reports as the basis for granting clearances. In response to our recommendation, DOD's November 2009 guidance that established RADAR also outlines the minimum documentation requirements adjudicators must adhere to when documenting personnel security clearance determinations for cases with potentially damaging information. In addition, DOD issued guidance in March 2010 that clarifies when adjudicators may use incomplete investigative reports as the basis for granting clearances. This guidance provides standards that can be used for the sufficient explanation of incomplete investigative reports.

## Metrics Not Yet Implemented to Measure Clearance Reciprocity

While some efforts have been made to develop quality metrics, agencies have not yet implemented metrics for tracking the reciprocity of personnel security clearances, which is an agency's acceptance of a background investigation or clearance determination completed by any authorized investigative or adjudicative executive branch agency. Although executive branch agency officials have stated that reciprocity is regularly granted, as it is an opportunity to save time as well as reduce costs and investigative workloads, we reported in 2010 that agencies do not consistently and comprehensively track the extent to which reciprocity is

[21]GAO, *DOD Personnel Clearances: Comprehensive Timeliness Reporting, Complete Clearance Documentation, and Quality Measures Are Needed to Further Improve the Clearance Process*, GAO-09-400 (Washington, D.C.: May 19, 2009).

granted government-wide.[22] ODNI guidance requires, except in limited circumstances, that all Intelligence Community elements "accept all in-scope[23] security clearance or access determinations." Additionally, Office of Management and Budget guidance[24] requires agencies to honor a clearance when (1) the prior clearance was not granted on an interim or temporary basis; (2) the prior clearance investigation is current and in-scope; (3) there is no new adverse information already in the possession of the gaining agency; and (4) there are no conditions, deviations, waivers, or unsatisfied additional requirements (such as polygraphs) if the individual is being considered for access to highly sensitive programs.

While the Performance Accountability Council has identified reciprocity as a government-wide strategic goal, we have found that agencies do not consistently and comprehensively track when reciprocity is granted, and lack a standard metric for tracking reciprocity.[25] Further, while OPM and the Performance Accountability Council have developed quality metrics for reciprocity, the metrics do not measure the extent to which reciprocity is being granted. For example, OPM created a metric in early 2009 to track reciprocity, but this metric only measures the number of investigations requested from OPM that are rejected based on the existence of a previous investigation and does not track the number of cases in which an existing security clearance was or was not successfully honored by the agency. Without comprehensive, standardized metrics to

[22]In addition to establishing objectives for timeliness, the Intelligence Reform and Terrorism Prevention Act of 2004 established requirements for reciprocity, which is an agency's acceptance of a background investigation or clearance determination completed by any authorized investigative or adjudicative executive branch agency, subject to certain exceptions such as completing additional requirements like polygraph testing. Further, in October 2008, ODNI issued guidance on the reciprocity of personnel security clearances. ODNI, Intelligence Community Policy Guidance 704.4, *Reciprocity of Personnel Security Clearance and Access Determinations* (Oct. 2, 2008).

[23]Although there are broad federal investigative guidelines, the details and depth of an investigation varies by agency depending upon its mission.

[24]Office of Management and Budget, *Memorandum for Deputies of Executive Departments and Agencies: Reciprocal Recognition of Existing Personnel Security Clearances* (Dec. 12, 2005); Office of Management and Budget, *Memorandum for Deputies of Executive Departments and Agencies: Reciprocal Recognition of Existing Personnel Security Clearances* (July 17, 2006).

[25]GAO, *Personnel Security Clearances: Progress Has Been Made to Improve Timeliness but Continued Oversight Is Needed to Sustain Momentum*, GAO-11-65 (Washington, D.C.: Nov. 19, 2010).

track reciprocity and consistent documentation of the findings, decision makers will not have a complete picture of the extent to which reciprocity is granted or the challenges that agencies face when attempting to honor previously granted security clearances.

In 2010, we reported that executive branch officials routinely honor other agencies' security clearances, and personnel security clearance information is shared between OPM, DOD, and, to some extent, Intelligence Community databases.[26] However, we found that some agencies find it necessary to take additional steps to address limitations with available information on prior investigations, such as insufficient information in the databases or variances in the scope of investigations, before granting reciprocity. For instance, OPM has taken steps to ensure certain clearance data necessary for reciprocity are available to adjudicators, such as holding interagency meetings to determine new data fields to include in shared data. However, we also found that the shared information available to adjudicators contains summary-level detail that may not be complete. As a result, agencies may take steps to obtain additional information, which creates challenges to immediately granting reciprocity.

Further, in 2010 we reported that because there is no government-wide standardized training and certification process for investigators and adjudicators, according to agency officials, a subject's prior clearance investigation and adjudication may not meet the standards of the inquiring agency. Although OPM has developed some training, security clearance investigators and adjudicators are not required to complete a certain type or number of classes. As a result, the extent to which investigators and adjudicators receive training varies by agency. Consequently, as we have previously reported, agencies are reluctant to be accountable for investigations and/or adjudications conducted by other agencies or organizations.[27] To achieve fuller reciprocity, clearance-granting agencies seek to have confidence in the quality of prior investigations and adjudications.

[26]GAO-11-65.

[27]GAO, *Personnel Clearances: Key Factors to Consider in Efforts to Reform Security Clearance Processes*, GAO-08-352T (Washington, D.C.: Feb. 27, 2008).

Consequently, we recommended in 2010 that the Deputy Director of Management, Office of Management and Budget, in the capacity as Chair of the Performance Accountability Council, should develop comprehensive metrics to track reciprocity and then report the findings from the expanded tracking to Congress. Although OMB agreed with our recommendation, a 2011 ODNI report found that Intelligence Community agencies experienced difficulty reporting on reciprocity. The agencies are required to report on a quarterly basis the number of security clearance determinations granted based on a prior existing clearance as well as the number not granted when a clearance existed. The numbers of reciprocal determinations made and denied are categorized by the individual's originating and receiving organizational type: (1) government to government, (2) government to contractor, (3) contractor to government, and (4) contractor to contractor. The report stated that data fields necessary to collect the information described above do not currently reside in any of the datasets available and the process was completed in an agency specific, semi-manual method. Further, the Deputy Assistant Director for Special Security of the Office of the Director of National Intelligence noted in testimony in June 2012 that measuring reciprocity is difficult, and despite an abundance of anecdotes, real data is hard to come by. To address this problem, ODNI is developing a web-based form for individuals to submit their experience with reciprocity issues to the ODNI. According to ODNI, this will allow them to collect empirical data, perform systemic trend analysis, and assist agencies with achieving workable solutions.

## Sustained Leadership Needed to Fully Develop and Implement Metrics to Monitor and Track Quality

As previously discussed, DOD accounts for the majority of security clearances within the federal government. We initially placed DOD's personnel security clearance program on our high-risk list[28] in 2005 because of delays in completing clearances.[29] It remained on our list until 2011 because of ongoing concerns about delays in processing clearances and problems with the quality of investigations and adjudications. In February 2011, we removed DOD's personnel security

[28]Every two years at the start of a new Congress, GAO issues a report that identifies government operations that are high risk due to their vulnerabilities to fraud, waste, abuse, and mismanagement, or are most in need of transformation to address economy, efficiency, or effectiveness.

[29]GAO, *High-Risk Series: An Update*, GAO-05-207 (Washington, D.C.: Jan. 1, 2005).

clearance program from our high-risk list largely because of the department's demonstrated progress in expediting the amount of time processing clearances.[30] We also noted DOD's efforts to develop and implement tools to evaluate the quality of investigations and adjudications.

Even with the significant progress leading to removal of DOD's program from our high-risk list, we noted in June 2012 that sustained leadership would be necessary to continue to implement, monitor, and update outcome-focused performance measures. The initial development of some tools and metrics to monitor and track quality not only for DOD but government-wide were positive steps; however, full implementation of these tools and measures government-wide have not yet been realized. While progress in DOD's personnel security clearance program resulted in the removal of this area from our high-risk list, significant government-wide challenges remain in ensuring that personnel security clearance investigations and adjudications are high-quality.

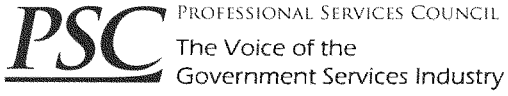
In conclusion, oversight of the reform efforts to measure and improve the quality of the security clearance process—including background investigations—are imperative next steps. Failing to do so increases the risk of damaging, unauthorized disclosures of classified information. The progress that was made with respect to expediting the amount of time processing clearances would not have been possible without committed and sustained congressional oversight and the leadership of the Performance Accountability Council. Further actions are needed now to fully develop and implement metrics to oversee quality at every step in the process. Chairman Carper, Ranking Member Coburn, this concludes my prepared statement. I would be pleased to answer any questions that you or other Members of the Committee may have at this time.

## GAO Contacts and Acknowledgment

For further information on this testimony, please contact Brenda S. Farrell, Director, Defense Capabilities and Management, who may be reached at (202) 512-3604 or farrellb@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this statement. GAO staff who made key contributions to

[30]GAO, *High-Risk Series: An Update*, GAO-11-278 (Washington, D.C.: Feb. 2011).

this testimony include Lori Atkinson (Assistant Director), Darreisha Bates, Renee Brown, John Van Schaik, and Michael Willems.




Statement for the Record of the
Professional Services Council

"The Navy Yard Tragedy: Examining Government
Clearances and Background Checks"

U.S. Senate
Homeland Security and Governmental Affairs
Committee

October 31, 2013

4401 Wilson Boulevard, Suite 600, Arlington, Virginia 22203 P. 703.875.8059 F. 703.875.8922 www.pscouncil.org

PSC commends the Senate Homeland Security and Governmental Affairs Committee for holding this hearing on federal security clearances and appreciates the opportunity to provide a written statement for the record.[1] The very foundation of this hearing is underpinned by the tragedy of September 16th and all of us at PSC express our deepest condolences to the families and friends of the federal civilian, contractor, military and law enforcement officials who lost their lives, and our wishes for a speedy recovery to those who were injured. We owe it to all of the victims and their families to determine, to the extent we can, why this tragedy occurred and, even more importantly, how future occurrences can be deterred, detected, and defused.

We also extend our deep gratitude to the extraordinary law enforcement personnel who responded so quickly and effectively in the face of imminent danger and to all those who showed extraordinary courage in the face of such horror. Those actions continue even today as the whole Navy family—including its military, civilians and contractors—work together to return to business.

COMPREHENSIVE REVIEW NEEDED

This singular incident at the Navy Yard is not all that should drive the need for a comprehensive review. The tragic 2009 shooting at Ft. Hood committed by Army Major Nidal Hassan, as well as the information security breaches perpetrated by Army Private Bradley Manning and contractor Edward Snowden, further highlight that a review of security clearance and facilities access processes and standards is necessary. The totality of these events further demonstrate that reviews being undertaken by Congress, the military, and the administration should focus on all aspects of the processes or standards and any deficiencies they may have. As you know, these standards and processes are equally applied to both government and contractor personnel. We believe that the DoD, Navy and OMB reviews have such a comprehensive, multi-sector focus, and should be completed before remedial actions are offered.

Simply, focusing solely on one sector, such as federal contractors, for example, would thus be inadequate. As these reviews continue, it is important that the effort remain focused on a thoughtful, thorough and fact-based assessment of the entire process to identify how and where it might be improved and whether any such improvement in the process could have prevented the September 16 event or any of the other events mentioned. It is also important that policy-makers understand some key facts about the security clearance and facilities access processes and that all stakeholders be involved in the discussion. After all, it is paramount to ensure both the well-being of all sectors that make up the whole of government and the protection of sensitive information that resides on government, contractor, and commercial systems.

---

[1] For 40 years, PSC has been the leading national trade association of the government professional and technical services industry. PSC's more than 370 member companies represent small, medium, and large businesses that provide federal agencies with services of all kinds, including information technology, engineering, logistics, facilities management, operations and maintenance, consulting, international development, scientific, social, environmental services, and more. Together, the association's members employ hundreds of thousands of Americans in all 50 states.

In addition, on June 20, 2013, two of the committee's subcommittees held a hearing on the security clearance procedures relating to the Edward Snowden disclosure of classified information.[2] Although only government officials testified at that hearing, we believe that hearing record provides valuable factual information to help inform this committee and the Congress in this review.

COMMON MISUNDERSTANDINGS ABOUT SECURITY CLEARANCES

Before discussing potential reforms, it is important to address some common misunderstandings or mythologies about the federal security clearance process.

First, many believe that federal contractors are subject to different security clearance standards and processes than federal employees. The fact is that the process for contractors and federal employees is exactly the same for the same level of clearance sought. It begins with the relevant federal agency—whether as a direct employer or, in the case of a contractor, the contracting agency—making a determination about the workforce skills it needs and then identifying the appropriate level of security clearance (confidential, secret, or top secret) required for the performance of such work, regardless of whether that work is being performed under contract or by in-house personnel. The decisions about whether and what level of security clearance is necessary are always made by a government official and never by a contractor. Beyond this initial identification step, the process then generally follows two major steps, the investigation and the adjudication—each of which includes specific milestones and out-year requirements for reevaluation.

Second, background investigations are performed according to the policies and procedures established by the Office of Personnel Management (OPM) or the Defense Security Service (DSS). Furthermore, the extent of the background investigation varies with the level of clearance required. Aaron Alexis, for example, held a secret-level clearance that he received in 2008 while working as a Navy reservist and, with the Navy's permission, he was able to retain that clearance when he transitioned to the private sector to work as a contractor on a Navy assignment that required a secret security clearance. Absent adverse, factual information being made available to government officials suggesting the need for an earlier review, secret clearances only require a periodic reinvestigation every 10 years, while top secret clearances require reinvestigation every 5 years.

Third, while OPM and DSS contract with a small number of companies to handle a portion of their background investigation workload, all of the contractors (and the government employees who also conduct background investigations) are required to follow government-mandated processes for conducting those investigations, and all of the investigative files, whether conducted by contractors or federal employees, are sent to OPM for an independent review for completeness and compliance with the OPM standards. Mr. Alexis' 2007 background investigation was conducted by one of the contractors

[2] See June 20, 2013 hearing by the Subcommittee on the Efficiency and Effectiveness of Federal Programs and the Federal Workforce and the Subcommittee on Financial and Contracting Oversight of the Committee on Homeland Security and Government Affairs Committee. Information about the hearing is available at http://www.hsgac.senate.gov/subcommittees/fpfw/hearings/examining-the-workforce-of-the-us-intelligence-community-and-the-role-of-private-contractors.

and, according to recent public statements from OPM, there is no indication that there was any failure to follow the dictated federal background investigation procedures. Today approximately 30 percent of all investigations are performed primarily by OPM or DSS federal employees, while the remainder is performed under contract. Every company and every employee conducting those background investigations is accountable for complying with the strict procedures established and held accountable for their actions. When allegations of wrong-doing do arise, it is important that the company and any individuals be given the opportunity to respond to the allegations made against them. While a recent OPM Inspector General report on fraudulent background checks suggests that there were unacceptable actions on the part of contractor personnel performing background investigations, the same report shows that 60 percent of known cases of impropriety involve in-house federal civilian government investigators. The point is not to denigrate federal employees but to demonstrate the need to assess the entire process regardless of who is conducting the reviews or seeking the clearance. In short, to the extent there have been fraudulent or incomplete background investigations, it is clear that the problem is unrelated to the question of whether the work was performed under contract or inside the government.

Finally, the adjudication—the analysis of information collected during the investigation and used for making the final determination according to presidentially established criteria of whether a clearance is to be granted, suspended or revoked—is performed ONLY by trained government personnel.

PRIOR SECURITY CLEARANCE REFORM EFFORTS

Any review of the current security clearance process should pay close attention to past efforts to reform the clearance process. Most notably, such efforts have focused on improving quality, timeliness, and efficiency. The need for past reforms were amplified following the September 11 terrorist attacks when demand for clearances was on the rise, yet the backlog for completing the process was significant and reviews were taking, in some cases, upwards of 400 days for a number of years prior to this seminal event. This inefficiency resulted in the security clearance process being included in GAO's High Risk List for several consecutive years. Congress generally, and several former members of this committee in particular, expressed serious concern about that backlog and in 2004 helped to shepherd to enactment the Intelligence Reform and Terrorism Prevention Act (IRTPA, P.L. 108-458) which set aggressive goals for 90 percent of security clearance determinations to be completed within 60 days. By 2010, the backlog had been greatly reduced as a result of process modernizations and, in 2011, the security clearance process was removed from the GAO High Risk List.

While the reforms were needed and widely supported, it is important to understand that they created substantial pressure to process clearances quickly. The OPM Inspector General has made clear that non-compliant investigations were and are exceptionally rare, and thus no evidence exists that the quality of the process was broadly sacrificed in the name of speed. Nonetheless, these dynamics cannot be ignored during these reviews.

It's also important to recognize that reforms may be achievable without reverting to the days of lengthy delay. For example, reciprocity among federal agencies, i.e. the acceptance of a security clearance

determination by one agency when a suitability determination has been made by another federal agency, has for many years been an issue that has added to delays in granting clearances. Again, the IRTPA, as well as an Executive Order by President George W. Bush, sought to spur greater reciprocity among the federal agencies. Regrettably, even after significant intra-governmental effort, meaningful reciprocity remains elusive. If true reciprocity could be achieved, further improvements to the approval timeframes could result. While reciprocity itself will not directly result in a higher quality process or standards, it could free up resources which could be dedicated to conducting more thorough investigations and adjudications.

In response to this obstacle, PSC, in conjunction with another association, developed the concept of the "Four Ones" of security clearances: one application, one investigation, one adjudication and one clearance.

FACILITIES ACCESS

Unrelated to the Navy Yard tragedy is the process used by the Navy to grant facilities access to commercial vendors who do not need a security clearance. This was highlighted by a DoD Inspector General report that was issued in draft form to congressional offices a few days before the September 16 event and publicly released in redacted form by the DoD IG several days later. While the security clearance and facilities access processes are intertwined, it is doubtful that more aggressive or restrictive facility security would have averted the Navy Yard events because Mr. Alexis had a valid reason to be at the Navy Yard that morning and had a valid, active security clearance that provided him valid access to Building 197. Nevertheless, had procedures required all personnel who enter federal facilities to go through metal detectors or have their baggage subjected to search—similar to the screening that all visitors and staff have to do at any of the entrances to the Capitol or the House or Senate office buildings—the ability to smuggle in weapons would be significantly diminished and likely deterred or detected. At the same time, however, as Navy officials have made clear, subjecting every individual and vehicle entering a facility to a full search, while an appealing thought, could prove entirely impractical.

Further, much of the DoD IG report focused on their discovery that several dozen individuals with criminal records gained access to the Navy Yard. These individuals were almost all personnel making routine deliveries to the base. It is not at all clear that the government could, or, even should, attempt to limit such access only to individuals with untarnished records. The complexity of doing so and the challenges associated with determining what types of incidents or timeframes would disqualify such individuals from making such deliveries, not to mention the disruptions and costs involved, are all important factors to be considered as needed improvements and enhancements to facility security are contemplated.

INTERIM ACTIONS

We have offered our expertise to the Navy, to DoD and to the Office of Management and Budget as they conduct their various reviews of the Navy Yard incident and potential remedial actions. The Navy has

already taken action to change the level of decision-making for certain types of disciplinary actions. In our view, there are other interim actions that can be taken by federal agencies to address some of the issues that have become public in the Alexis case relating to security clearances.

One key area for reform should be the mechanisms, or lack thereof, for information disclosure and sharing regarding anyone who already has a clearance. For example, there is no government-wide federal database that contains information about individual arrest records by state and local law enforcement entities. If such a system, or system of systems, existed, it could enable creation of an alert mechanism to inform federal agencies if one of their cleared employees or contractors was arrested but not convicted after a clearance has been granted, regardless of whether that information was voluntarily disclosed by the security clearance holder. While privacy and due process issues must be considered prior to the implementation of such a tool, the idea should be part of the broad discussion.

We would also support evaluating the merits of reducing the timeframe for a periodic reinvestigation of a secret clearance from the current ten years. But while shortening the time period for such periodic reinvestigation may help identify issues that arise after the last background investigation and clearance approval, it also adds significant cost and resource burdens to federal agencies and to the federal adjudicators. For example, the committee may be aware that, in June 2013, the DSS suspended periodic reinvestigations for contractor top secret clearances because of budgetary constraints. While those reinvestigations were restarted in August, there is no indication that the budgetary resources or human capital necessary to conduct more reinvestigations is or will become available.

We would also support a more thorough review of the positions that require security clearances and the level of clearances required. According to the 2012 security clearance census report from the Director of National Intelligence, the federal executive agent for national security clearances, more than 5 million people hold security clearances at all levels but only 1.06 million of those are contractors. Certainly it would be advantageous to reduce, to the appropriate extent, the over-classification of documents and the number of individuals who require clearances.

CONCLUSION

The horrific events at the Washington Navy Yard require a prompt, thorough and informed review of the events leading up to that tragedy and the security clearance and facilities access processes. But in order to be effective, those reviews must evaluate all elements and involve all of the stakeholders affected. PSC has offered our assistance to this committee, to other congressional inquiries and to the Executive Branch, to find appropriate, effective and sustainable changes.

Thank you for the opportunity to provide our views.

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

The Director

OCT 31 2013

The Honorable Tom Coburn, M.D.
Ranking Member
Homeland Security and Governmental Affairs
United States Senate
340 Dirksen Senate Office Building
Washington, DC 20510

Dear Ranking Member Coburn:

Thank you for providing the U.S. Office of Personnel Management (OPM) the opportunity to testify at today's hearing "The Navy Yard Tragedy: Examining Government Clearances and Background Checks." I am writing to clarify a response that I provided during today's testimony. You asked whether OPM contractors provide quality reviews of investigations performed by OPM contractors, and whether the same contractor conducts the review that conducted the background investigation.

As I stated during the hearing, the contractors that conduct fieldwork are contractually required to conduct a quality review of their work before forwarding it to OPM, where the work receives another OPM "in-house" review. All Top Secret investigations are reviewed by Federal employees. Secret investigations, however, may be reviewed either by Federal employees or by OPM contract employees depending on the complexity of the investigation. Thus, some less complex investigations for secret clearances are subject to a routine quality review by contract employees (rather than Federal employees). Such investigations, although reviewed for quality by contract employees, are subject to audits conducted by Federal employees.

I apologize for the lack of clarity and precision in the answer I provided at the hearing and look forward to receiving additional questions from you and the Committee.

Sincerely,

Elaine Kaplan
Acting Director

cc: The Honorable Thomas Carper, Chairman
Committee on Homeland Security and Governmental Affairs, United States Senate

# U.S. Office of Personnel Management (OPM)
# Federal Investigative Services Division (FIS)

## WHITE PAPER

## Support Services Contract
## Cost Benefit Analysis

Support Services Contract Cost Benefit Analysis

## Purpose

During a Senate Homeland Security and Government Affairs Committee hearing, held jointly by the Financial and Contracting Oversight Subcommittee and the Efficiency and Effectiveness of Federal Programs and the Federal Workforce Subcommittee, on June 20, 2013, one of the Chairs of the Subcommittees requested to have FIS do a cost benefit analysis (CBA) to determine if the Support Services Contract (SSC) held by U.S. Investigations Services Inc. (USIS) was financially beneficial to the Federal Government as compared to hiring federal employees to conduct the same work.

This white paper (1) describes the methodology OPM used to compare costs and (2) OPM's analysis of results. In preparing this paper, OPM has sought to (1) capture the full costs of government and private sector performance and (2) provide "like comparisons" of costs that are of a sufficient magnitude to influence the final decision on the most cost effective source of support for the organization. These principles are laid out in OMB Memorandum M-09-26, which provides government-wide management guidance to agencies for managing the multi-sector workforce.

See: http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_fy2009/m-09-26.pdf at Attachment I.B.2.

Application of the methodology described below suggests that it is cost effective to continue using contract support to perform a portion of the background investigation work, with the balance continuing to be performed by federal employees. Notwithstanding this finding, OPM intends to continually analyze this mix -- both from a cost and human capital perspective. Among other things, OPM will work with OMB as it develops government-wide guidance on cost-comparisons and intends to revisit its analysis based on any alternative methodologies that may result from this effort as well as based on any other programmatic changes that may be made over time to its approach to performing background investigations.

## Methodology

This section outlines the methodology used to conduct a CBA of the SSC for OPM-FIS. The goal of the methodology is to determine an equivalent basis to compare the projected costs of the SSC with the projected costs if performed by Federal staff. The first step is to develop cost estimates of the SSC as detailed in the following section.

### SSC Costs

To determine SSC costs, a series of steps were undertaken. Summary of costs are:

Support Services Contract Cost Benefit Analysis

| Fiscal Yr | Costs |
|---|---|
| FY2011 | $ 53.93 M |
| FY2012 | $ 46.21 M |
| FY2013 | $ 46.02 M |
| FY2014 | $ 47.35 M |
| FY2015 | $ 48.71 M |

**Table 1 – Actual and Projected Support Services Contract Costs*[1]**
*Note Q4 FY 2013 – FY 2015 costs are projected

**STEP 1:** The actual costs were retrieved from beginning FY 2011 through Q3 FY 2013. The remainder of FY 2013 was straight-line projected based on the actual costs from 10/1/2012 – 6/30/2013. See Table 2, below, illustrating this calculation.

| FY2013 Actuals (FY13 Q1 - Q3) | Average per Month (FY13 Q1 - Q3) | FY 2013 Q4 Estimate | FY2013 Projected Total |
|---|---|---|---|
| $ 34.51 M | $ 3.83 M | $ 11.50 M | $ 46.02 M |

**Table 2 – FY 2013 Q1-Q3 Actual Costs with Q4 Projection[1]**

**STEP 2:** To project the costs for FY 2014 and FY 2015, the Support Services Contract document was referenced to calculate an average percentage increase per FY. This increase was based upon the line item prices for each product. The percentage change was first calculated for Fiscal Years 2013 – 2014 (2.80% increase), and then for Fiscal Years 2014 - 2015 (2.98% increase). The percentage change was averaged over those time periods to arrive at an overall average of 2.89%. See Table 3, below, illustrating the calculations.

| Fiscal Year | Average % Increase |
|---|---|
| FY 2013 - FY2014 | 2.80% |
| FY 2014 - FY2015 | 2.98% |
| **Overall Average** | **2.89%** |

**Table 3 – Average percentage change in pricing[1]**

**STEP 3:** The overall average percentage change (2.89%) was then used to project SSC costs for FY 2014 and FY 2015. Table 4 illustrates the actual and projected costs.

| Fiscal Yr | Costs |
|---|---|
| FY2011 | $ 53.93 M |
| FY2012 | $ 46.21 M |
| FY2013 | $ 46.02 M |
| FY2014 | $ 47.35 M |
| FY2015 | $ 48.71 M |

**Table 4 – SSC Actual & Projected Costs**[1]

The costs illustrated in Table 4 were used as the basis for comparison with the Federal Costs. The methodology to determine the Federal costs will be examined next.

**Federal Costs**

To determine Federal Costs, a series of steps were undertaken to develop an equivalent basis for comparison.

**STEP 1:** Personnel data for the Support Services Contract with the position-by-position description and the total number of Contractor Manpower Equivalent (CME) is shown in Table 6 below. For comparison purposes, using the provided position descriptions (and other data provided by the support contractor), equivalent Federal positions were determined. FY 2012 salaries were then applied according to General Schedule (GS) and Wage Grade (WG) scales (refer to Table 6 to see how SSC position descriptions relate to the Federal GS and WG scales).

**STEP 2:** Because the number of people in each type of position fluctuates significantly annually (as shown in table 5) an average CME for each position was calculated. The calculation was done by taking the average for each year (2010-2011 [867.5]; 2011-2012 [962.5]; 2012-2013 [996.0]) and then averaging these three periods to calculate an overall average (942). Table 5 summarizes this calculation for all positions.

| SSC Job Title | Actual | | | | Averages | | | |
|---|---|---|---|---|---|---|---|---|
| | 31-Dec-10 | 31-Dec-11 | 31-Dec-12 | 31-May-13 | 2010-2011 | 2011-2012 | 2012-2013 | 3 YR avg |
| Support Schedule Technician | 211 | 204 | 265 | 241 | 207.5 | 234.5 | 253.0 | **231.7** |
| Support File Technician | 133 | 131 | 186 | 165 | 132.0 | 158.5 | 175.5 | **155.3** |
| Support Imaging Technician | 80 | 91 | 88 | 92 | 85.5 | 89.5 | 90.0 | **88.3** |
| Support Pre-Review | 221 | 330 | 269 | 287 | 275.5 | 299.5 | 278.0 | **284.3** |
| Support Telephone Liaisons | 9 | 6 | 6 | 6 | 7.5 | 6.0 | 6.0 | **6.5** |
| Support Case Closing | 25 | 34 | 29 | 32 | 29.5 | 31.5 | 30.5 | **30.5** |
| Support Case Closing Automated | 9 | 12 | 12 | 12 | 10.5 | 12.0 | 12.0 | **11.5** |
| Support Post Closing | 18 | 17 | 16 | 13 | 17.5 | 16.5 | 14.5 | **16.2** |
| Support Mailroom Technician | 51 | 48 | 56 | 61 | 49.5 | 52.0 | 58.5 | **53.3** |
| Support Quality Control | 5 | 13 | 17 | 22 | 9.0 | 15.0 | 19.5 | **14.5** |
| Support Manager | 22 | 24 | 25 | 42 | 23.0 | 24.5 | 33.5 | **27.0** |
| Support Other | 19 | 22 | 24 | 26 | 20.5 | 23.0 | 25.0 | **22.8** |
| Sub Total Program FTE | **803** | **932** | **993** | **999** | **867.5** | **962.5** | **996.0** | **942.0** |

**Table 5 – CME/FTE average calculations**[4]

**STEP 3:** To make a valid comparison, we considered average CME totals as analogous to FTE totals. To calculate a FY 2012 base salary total for the Federal equivalent staff, the average FTE was multiplied by the GS or WG salary for each position. All positions were then totaled to derive a total base salary. The below example demonstrates how the base salary for one position was calculated.

> *EXAMPLE: The Federal equivalent for an Imaging Technician is GS-2 Step 1 (FY12 salary = $23,294). The overall CME average for this position is 46 FTE. Therefore, the total base salary cost for this position is $1.07M ($23,294 * 46 FTE).*

Table 6, below, illustrates the FY 2012 base salary for each position along with the total base salary ($31.46M).

| Federal Position / Support Contract Position | Step 1 Salary | Total FTE | Total Salary |
|---|---|---|---|
| **GS-2** | **$ 23,294** | **53.0** | **$ 1.23 M** |
| Imaging Technician | $ 23,294 | 46.0 | $ 1.07 M |
| Office Machine Operator | $ 23,294 | 7.0 | $ 0.16 M |
| **GS-3** | **$ 25,415** | **224.2** | **$ 5.70 M** |
| Data Support Clerk | $ 25,415 | 123.3 | $ 3.13 M |
| Mail Clerk | $ 25,415 | 48.8 | $ 1.24 M |
| Material Processing Technician | $ 25,415 | 32.8 | $ 0.83 M |
| Clerk | $ 25,415 | 9.0 | $ 0.23 M |
| Telephone Liasion | $ 25,415 | 6.5 | $ 0.17 M |
| ISD Security Monitor | $ 25,415 | 3.8 | $ 0.10 M |
| **GS-4** | **$ 28,532** | **223.5** | **$ 6.38 M** |
| Case Screening Technician | $ 28,532 | 207.7 | $ 5.93 M |
| Workload Leader | $ 28,532 | 4.4 | $ 0.13 M |
| Inv Record Techinician | $ 28,532 | 3.7 | $ 0.11 M |
| File Release Clerical | $ 28,532 | 3.7 | $ 0.11 M |
| Technical Associate | $ 28,532 | 3.0 | $ 0.09 M |
| *Ops Manager | $ 28,532 | 1.0 | $ 0.03 M |
| **GS-5** | **$ 31,921** | **28.3** | **$ 0.90 M** |
| Case Closing Technician | $ 31,921 | 11.5 | $ 0.37 M |
| Redaction Release Specialist | $ 31,921 | 10.3 | $ 0.33 M |
| Mail Support Technician | $ 31,921 | 2.5 | $ 0.08 M |
| Ops Manager | $ 31,921 | 2.0 | $ 0.06 M |
| Operations Assistant | $ 31,921 | 2.0 | $ 0.06 M |
| **GS-6** | **$ 35,582** | **52.5** | **$ 1.87 M** |
| Data Support Technician | $ 35,582 | 35.5 | $ 1.26 M |
| Corrections Tech | $ 35,582 | 15.0 | $ 0.53 M |
| Ops Manager | $ 35,582 | 2.0 | $ 0.07 M |

| Federal Position / Support Contract Position | Step 1 Salary | Total FTE | Total Salary |
|---|---|---|---|
| **GS-7** | **$ 39,541** | **303.6** | **$ 12.00 M** |
| Material Analyst I | $ 39,541 | 238.8 | $ 9.44 M |
| Support Services Team Leader | $ 39,541 | 30.0 | $ 1.19 M |
| Investigative Specialist SS | $ 39,541 | 18.5 | $ 0.73 M |
| Material Analyst II | $ 39,541 | 14.8 | $ 0.59 M |
| Ops Manager | $ 39,541 | 1.0 | $ 0.04 M |
| Quality Control Technician | $ 39,541 | 0.5 | $ 0.02 M |
| **GS-8** | **$ 43,791** | **7.0** | **$ 0.31 M** |
| Ops Manager | $ 43,791 | 7.0 | $ 0.31 M |
| **GS-9** | **$ 48,367** | **18.0** | **$ 0.87 M** |
| Reviewer | $ 48,367 | 9.7 | $ 0.47 M |
| Corrections Analyst | $ 48,367 | 5.0 | $ 0.24 M |
| PIC Specialist | $ 48,367 | 3.3 | $ 0.16 M |
| **GS-11** | **$ 58,519** | **10.3** | **$ 0.60 M** |
| Ops Manager | $ 58,519 | 7.0 | $ 0.41 M |
| Quality Assurance Team Leader | $ 58,519 | 2.3 | $ 0.13 M |
| Management Analyst | $ 58,519 | 1.0 | $ 0.06 M |
| **WG-5** | **$ 58,874** | **1.2** | **$ 0.07 M** |
| Warehouseman | $ 58,874 | 1.2 | $ 0.07 M |
| **GS-12** | **$ 70,141** | **16.5** | **$ 1.16 M** |
| Quality Assurance Specialist | $ 70,141 | 9.7 | $ 0.68 M |
| Senior Operations Manager | $ 70,141 | 3.0 | $ 0.21 M |
| Training Specialist | $ 70,141 | 2.8 | $ 0.20 M |
| Ops Manager | $ 70,141 | 1.0 | $ 0.07 M |
| **GS-13** | **$ 83,407** | **2.0** | **$ 0.17 M** |
| Quality Assurance Manager | $ 83,407 | 1.0 | $ 0.08 M |
| Training Manager | $ 83,407 | 0.5 | $ 0.04 M |
| Process Improvement Leader | $ 83,407 | 0.5 | $ 0.04 M |
| **GS-14** | **$ 98,562** | **0.8** | **$ 0.08 M** |
| SS Deputy Program Manager | $ 98,562 | 0.8 | $ 0.08 M |
| **GS-15** | **$ 115,937** | **1.0** | **$ 0.12 M** |
| Vice President Support Services | $ 115,937 | 1.0 | $ 0.12 M |
| **Grand Total** | | **941.9** | **$ 31.46 M** |

**Table 6 – Federal Equivalent and Support Contract positions with FY12 base salary information[2,3]**

**STEP 4:** Using the total FY 2012 base salary of $31.46M three additional measurements were applied to the Base Salary Cost to arrive at a Total Cost: 1) Benefits Rate (31.5%)[5]; 2) Overhead Rate (18.9%)[5]; and 3) Inflation Factor (2.5%). The Benefits Rate used is the current Fiscal Year benefits rate. The Overhead Rate used was derived from the FY 2012 OPM-FIS Cost Allocation Model (CAM) and is solely representative of overhead costs in FY 2012.

The Inflation Factor was assigned a value of 2.5%. Table 7, below, illustrates the FY2012 Base Salary Cost with these measurements applied. The Inflation Factor was used to project costs for FY 2013 – FY 2015.

| Step | Measurment | Amount | Calculation |
|---|---|---|---|
| 1 | Base Salary | $ 31.46 M | From Table 6 for FY 2012 |
| 2 | Benefit Cost | $ 9.91 M | Base Salary * Benefit Rate (31.5%) |
| 3 | Salary & Benefit Cost | $ 41.36 M | Base Salary + Benefit Cost |
| 4 | Overhead Cost | $ 7.82 M | Salary & Benefit Cost * Overhead Rate (18.9%) |
| 5 | FY12 Total Staff Cost | $ 49.18 M | Salary & Benefit Cost + Overhead Cost |
| 6 | FY13 Total Staff Cost | $ 50.41 M | FY12 Total Staff Cost * Inflation Factor (2.5%) |
| 7 | FY14 Total Staff Cost | $ 51.67 M | FY13 Total Staff Cost * Inflation Factor (2.5%) |
| 8 | FY15 Total Staff Cost | $ 52.96 M | FY14 Total Staff Cost * Inflation Factor (2.5%) |

**Table 7 – Total estimated Federal costs[2]**

**STEP 5:** The total Federal costs for Fiscal Years 2013-2015, were divided by the FTE number (942) to arrive at a normalized per FTE cost, per Fiscal Year. Normalizing the FTE was done to account for overall fluctuations in all staff and, in addition, fluctuations of staff within each contractor position type. As a result, OPM-FIS was able to derive the most accurate average cost per FTE. Table 8, below, illustrates the per FTE calculation.

| Fiscal Year | FTE | Total Staff Cost | Avg Staff Cost/FTE |
|---|---|---|---|
| FY 2013 | 942 | $ 50.41 M | $ 53,520.13 |
| FY 2014 | 942 | $ 51.67 M | $ 54,858.14 |
| FY 2015 | 942 | $ 52.96 M | $ 56,229.59 |

**Table 8 – Per FTE cost calculation[2]**

**STEP 6:** Once an accurate cost per FTE was derived in step 5, OPM-FIS needed to evaluate the optimal number of FTE needed to run a fully efficient and productive operation. According to the Technical Proposal of the Support Services Contract, the requisite CME needed to meet workload demands is 994 (current SSC staffing level is 999). Therefore, multiplying the normalized per FTE cost by994, provides the appropriate comparison of the costs generated by the SSC and the hypothetical costs generated by a similar Federal effort. Table 9, below, illustrates the total Federal equivalent costs for FY 2013 –FY 2015.

| Fiscal Year | Avg Staff Cost/FTE | FTE (per SSC Tech Proposal) | Total Staff Cost |
|---|---|---|---|
| FY 2013 | $ 53,520.13 | 994 | $ 53.20 M |
| FY 2014 | $ 54,858.14 | 994 | $ 54.53 M |
| FY 2015 | $ 56,229.59 | 994 | $ 55.89 M |

**Table 9 – Total Federal Equivalent Costs[2]**

The Analysis section will examine these differences next, but first, the assumptions made during this analysis will be addressed.

**Assumptions**

The methodology above includes several assumptions. They are as follows:

1) Based on the recent workload trends, we assumed workload will remain constant until contract expiration (FY 2015).
2) Costs compare only the years until expiration (FY 2015); years beyond contract expiration were not factored in (especially important for future Federal costs).
3) Federal personnel estimates will be one-to-one, rather than some existing SSC positions being absorbed by current organization structure.

## Analysis

| | Support Services Contract (SSC) | | | Federal Equivalent | | | Savings from Federal Equivalent | |
|---|---|---|---|---|---|---|---|---|
| | CME | Cost per CME | Total Cost | FTE | Cost per FTE | Total Cost | Cost per CME/FTE | Total Cost |
| FY 2013 | 994 | $ 46,293.52 | $ 46.02 M | 994 | $ 53,520.13 | $ 53.20 M | $ 7,226.61 | $ 7.18 M |
| FY 2014 | 994 | $ 47,631.83 | $ 47.35 M | 994 | $ 54,858.14 | $ 54.53 M | $ 7,226.31 | $ 7.18 M |
| FY 2015 | 994 | $ 49,008.82 | $ 48.71 M | 994 | $ 56,229.59 | $ 55.89 M | $ 7,220.77 | $ 7.18 M |
| Total | | | $ 142.08 M | | | $ 163.62 M | | $ 21.54 M |

**Table 10 – SSC Costs vs. Federal Costs**[6]

As explained in the last paragraph of the Methodology section, the normalized per FTE cost was multiplied by 994 to arrive at a basis for comparison with the SSC. Table 10, above, illustrates the results of the analysis.

According to the analysis, in FY 2013 a Federal Equivalent support function would cost $53.20M, which results in a $7.18M (16%) increase to current costs. Similar increases can be expected in FY 2014 ($7.18M) and FY 2015 ($7.18M). Overall, based on the methodology outlined above, it is estimated that from FY 2013 –FY 2015 total savings by continuation of the SSC as compared to a Federal Equivalent operation would be $21.54M.[1]

OPM used available data in calculating costs, such as benefits and overhead, so as not to over- or under-inflate costs. While OPM prefers to use factors shaped by available cost experience to the

[1] Another significant factor and important consideration is the additional federal retirement costs for added federal staff. While these costs may not directly show in OPM-FIS's bottom line, a cost would still be incurred within the Federal Government, which means the savings to the taxpayer from contract performance are likely to be larger than indicated by this methodology.

general assumption made in Circular A-76, it recognizes that the longstanding overhead rate (12%) and benefits rate (36.45%) in the Circular are different than that in OPM's model. For this reason, OPM performed additional analysis using the lower overhead rate and higher benefits rate to see if it affects the bottom-line conclusion. Table 11, below, summarizes the analysis with incorporated A-76 figures for benefits and overhead.

| | Support Services Contract (SSC) | | | Federal Equivalent | | | Savings from Federal Equivalent | |
|---|---|---|---|---|---|---|---|---|
| | CME | Cost per CME | Total Cost | FTE | Cost per FTE | Total Cost | Cost per CME/FTE | Total Cost |
| FY 2013 | 994 | $ 46,293.52 | $ 46.02 M | 994 | $ 52,311.98 | $ 52.00 M | $ 6,018.45 | $ 5.98 M |
| FY 2014 | 994 | $ 47,631.83 | $ 47.35 M | 994 | $ 53,619.78 | $ 53.30 M | $ 5,987.95 | $ 5.95 M |
| FY 2015 | 994 | $ 49,008.82 | $ 48.71 M | 994 | $ 54,960.27 | $ 54.63 M | $ 5,951.45 | $ 5.92 M |
| Total | | | $ 142.08 M | | | $ 159.93 M | | $ 17.85 M |

**Table 11 – SSC Costs vs. Federal Costs Applying A-76 Guidance**

OPM found that continued use of contract support would still provide savings over federal performance even using the A-76 rates -- i.e., $142.08M for contract performance from FYs 13-15 vs. $159.93M for performance by federal employees (a nearly 13% savings).

Having a portion of the background investigation function performed by contract support provides other benefits beyond that which is reflected in the figures above. Of particular note, contract support allows OPM to better manage the fluctuation in workload, since it can increase or decrease the amount of investigation work in real time that it tasks to the contractor. According to the SSC, beginning in FY 2012 through May 2013, personnel fluctuated from 824 to 994- a difference of 170 personnel.[7] Since the same flexibility to increase and decrease labor based on existing workload doesn't exist when using full-time federal employees, OPM would need to consider the cost impact if all background investigation work were performed by federal employees. For example, since FIS prices its products to fully recover the cost to produce those products, it could potentially need to raise prices to mitigate the risk and cover costs in situations where workload diminishes.

In short, OPM believes the above analysis supports the continued use of contract support as part of a strategy that relies on a mix of contract and federal employees to perform background investigations. However, as explained above, OPM intends to continually analyze its workforce mix, both from a cost and human capital perspective. It will revisit this cost analysis based on any alternative methodologies that may result from OMB's efforts to develop government-wide guidance on cost-comparisons as well as any other programmatic changes that may be made over time to its approach to performing background investigations.

In addition, OPM remains committed to ensuring that when work is performed by a contractor, there is effective oversight and management of the contractor's activities. This oversight is critical to holding contractors to the terms of their contract and making sure they act with appropriate business ethics and integrity. This oversight is also critical to making sure that the responsibilities of the contractor do not expand to include activities which are inherently governmental. For example, under any scenario involving performance by an SSC, OPM will

continue to ensure that all decisions on whether or not to grant a clearance shall be made only by government officials.

## References

1) Actual Support Costs were pulled from our Billing file via reporting software; Estimated Support Costs over the contract period were pulled from the SSC's Technical Proposal. Both costs were combined on an Excel spreadsheet – "ContractorCosts_by_CaseType_FY11-13_Final_20130709".
    a. The FY2013 projection is located in the spreadsheet "ContractorCosts_by_CaseType_FY11-13_Final_20130709", within the sheet called, "FY13-Data".
2) Federal calculations were derived using Microsoft Excel – "Fed_Data_Final_20130709".
3) WG Hourly information obtained in an email from OPM Human Resources – "USIS Support Positions GS Equivalents (WG Hourly Table)".
   WG Hourly to Salary conversion information obtained in an email from OPM Human Resources – "USIS Support Positions GS Equivalents (Salary Conversion)".
4) The Support Contractor Provided an Excel spreadsheet with personnel numbers – "USIS_Support_Staff 2008 to May 31 OPM Confidential_Final_20130709" (information is proprietary to contractor).
5) Benefits & Overhead Rates (obtained from FY12 Cost Allocation Model) calculated using Microsoft Excel – "Federal FTE cost calc_Final_20130709". The CAM identified non-labor overhead costs for FY 2012, including equipment, supplies, space, and other tasks related to headquarters management, accounting, human resources support, legal support, IT support, and similar common services performed external to but in support of the background investigation work performed within FIS.
6) The cost comparison of the SSC and the Federal effort was created using Microsoft Excel – "CBA Table_CostCompare_Final_20130709".
7) The Month-to-Month fluctuations were obtained from the SSC via an email – "SSC Month-to-Month Fluctuations".

**Post-Hearing Questions for the Record**
**Submitted to the Honorable Joseph G. Jordan**
**"The Navy Yard Tragedy: Examining Government Clearances and Background Checks"**
**October 31, 2013**

## Chairman Carper

1. **GAO's 2012 Annual Report on Opportunities to Reduce Duplication, Overlap, and Fragmentation identified personnel background investigations as an area where OMB should take action to prevent agencies from making potentially duplicative investments in electronic case management and adjudication systems. In this report, GAO noted that seven different agencies had made investments in electronic systems that had potentially duplicative capabilities for case management and adjudication. GAO also reported that the Performance Accountability Council has not developed specific government wide guidance regarding how agencies should leverage existing technologies to prevent agencies from making duplicative investments in electronic case management and adjudication systems.**

    a. **What is the executive branch doing to prevent duplicative efforts to enhance the automation of the security clearance process?**

OMB continues to work with the Executive Agents to issue guidance to reduce duplication as agencies develop and improve electronic case management systems, adjudication tracking systems, and continuous evaluation technologies in support of suitability and personnel security clearance processes. For example, in May 2012, the Department of Defense (DoD) directed the consolidation of the seven non-Intelligence Community (IC) DoD Central Adjudication Facilities, to include DoD-wide Suitability and HSPD-12 adjudications under a single centralized authority. This consolidation effort has made considerable progress, and DoD continues to work towards efficiently allocating adjudicative resources in a single case management system. The Performance Accountability Council, the Security Executive Agent, and DoD continue to promote automation and information sharing to the greatest extent possible. Progress has been made by leveraging new technologies resulting in the development and deployment of eQIP and eAdjudication. Moreover, the President has directed OMB to conduct a 120-day review of Federal employee suitability and contractor fitness determinations as well as security clearance procedures. The review will identify potential vulnerabilities in Government policies, programs, processes, and procedures involving determinations of Federal employee suitability, contractor fitness, and general personnel security. As part of the scope of this review, areas of duplication and inefficiencies that exist in our current processes will also be examined. The release of findings and recommendations is scheduled for the end of February 2014.

**b. How do the leaders of the reform effort ensure that agency information technology systems have the ability to share necessary information and avoid duplication?**

As mentioned above, some progress has been made to improve the interoperability of security and suitability IT systems. The leaders of the Reform Effort are all directly involved in the ongoing 120 Day Suitability and Security Review process. Improving information sharing of information relevant to adjudications as it becomes available while reducing duplication in our current processes is a top priority of this Review, as is avoiding duplication as we explore IT capabilities and potential solutions related to the transition from our current five or ten year periodic reevaluation model to a more continuous evaluation model.

**2. What do you see as remaining barriers to agencies providing reciprocity to security clearances granted by other agencies?**

In a previous report, GAO recommended that in order to further improve Government-wide reciprocity, the Deputy Director of Management, Office of Management and Budget, in the capacity as Chair of the Performance Accountability Council, develop comprehensive metrics to track reciprocity and then report the findings from the expanded tracking to Congress. The Security Executive Agent is preparing his response to a request from Senator Dianne Feinstein, Chairman of the Select Committee on Intelligence and Senator Saxby Chambliss, Vice Chairman on the status of the strategy and timeline for carrying out reciprocity requirements mandated in section 300a(d) of the *Intelligence Reform and Terrorism Prevention Act 2004* (50 U.S.C435b(d). OMB and the Performance Accountability Council through the efforts of the 120 Day Review will work with the Security Executive Agent to develop these additional reciprocity metrics. GAO has stated that they are encouraged by the Performance Accountability Council's work to develop quality metrics, which include some metrics for tracking reciprocity. The ODNI, OPM, and DoD-led interagency Quality Assessments Working Group, which was stood up in 2012, continues their work to define "quality" in the background investigation process. The outcome of that working group's efforts will be endorsed by the Performance Accountability Council and signed out in policy by the Executive Agents. As a result of improved quality of a background investigation, reciprocal acceptance of the investigation should also improve.

## Senator Coburn

**1. GAO's 2012 Annual Report on Opportunities to Reduce Duplication, Overlap, and Fragmentation identified personnel background investigations as an area where OMB should take action to prevent agencies from making potentially duplicative investments in electronic case management and adjudication systems. In this report, GAO noted that seven different agencies had made investments in electronic systems that had potentially duplicative capabilities for personnel security clearance case management and adjudication.**
**These agencies include:**

- **Department of Defense**
- **National Reconnaissance Office**
- **Department of the Treasury**
- **Office of Personnel Management**
- **Department of Justice**
- **Department of Homeland Security**
- **Department of Veterans Affairs**

a. **Why are these seven agencies duplicating each other's efforts in electronic case management and adjudication systems?**

OMB continues to work with the Executive Agents to issue guidance to reduce duplication as agencies develop and improve electronic case management systems, adjudication tracking systems, and continuous evaluation technologies in support of suitability and personnel security clearance processes. For example, in May 2012, DoD directed the consolidation of the seven non-Intelligence Community (IC) DoD Central Adjudication Facilities, to include DoD-wide Suitability and HSPD-12 adjudications under a single centralized authority. This consolidation effort has made considerable progress, and DoD continues to work towards efficiently allocating adjudicative resources in a single case management system. The Performance Accountability Council, the Security Executive Agent, and DoD continue to promote automation and information sharing to the greatest extent possible. Progress has been made by leveraging new technologies resulting in the development and deployment of eQIP and eAdjudication. While some considerable progress has been made, there is still much work to be done. The President has directed OMB to conduct a 120-day review of Federal employee suitability and contractor fitness determinations as well as security clearance procedures. The review will identify potential vulnerabilities in Government policies, programs, processes, and procedures involving determinations of Federal employee suitability, contractor fitness, and general personnel security. As part of the scope of this review, areas of duplication and inefficiencies that exist in our current processes will also be examined. The release of findings and recommendations is scheduled for the end of February 2014.

b. **What is OMB, specifically the Deputy Director for Management in his capacity as chair of the Performance Accountability Council, doing to prevent duplicative efforts to enhance the automation of the security clearance process?**

Please see the response to 1.a above.

c. **What steps is OMB taking to ensure that agency information technology systems have the ability to share necessary information and avoid duplication during the personnel security clearance process?**

As mentioned above, some progress has been made to improve the interoperability of security and suitability IT systems. The leaders of the Reform Effort are all directly involved in the ongoing 120 Day Suitability and Security Review process. Improving information sharing of information relevant to adjudications as it becomes available while reducing duplication in our current processes is a top priority of this Review, as is avoiding duplication as we explore IT capabilities and potential solutions related to the implementation of a continuous evaluation program to provide near real-time access to automated adjudicatively relevant information.

**2. GAO also reported that the Performance Accountability Council has not developed specific government-wide guidance regarding how agencies should leverage existing technologies to prevent agencies from making duplicative investments in electronic case management and adjudication systems.**

a. **What is OMB, specifically the Deputy Director for Management in his capacity as chair of the Performance Accountability Council, doing to prevent duplicative efforts to enhance the automation of the security clearance process?**

Please see the response to 1.a above.

b. **What steps is OMB taking to ensure that agency information technology systems have the ability to share necessary information and avoid duplication during the personnel security clearance process?**

As mentioned above, some progress has been made to improve the interoperability of security and suitability IT systems. The leaders of the Reform Effort are all directly involved in the ongoing 120 Day Suitability and Security Review process. Improving information sharing of information relevant to adjudications as it becomes available while reducing duplication in our current processes is a top priority of this Review, as is avoiding duplication as we explore IT capabilities and potential solutions related to the implementation of a continuous evaluation program to provide near real-time access to automated adjudicatively relevant information.

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT

**Post-Hearing Questions for the Record**
**Submitted to the Honorable Elaine D. Kaplan**
**From Senator Thomas R. Carper**

**"The Navy Yard Tragedy: Examining Government Clearances and Background Checks"**
**October 31, 2013**

1. **Please discuss the steps that OPM takes to monitor the quality of the investigative products it provides customer agencies. Specifically, how does OPM monitor and review the quality and completeness of investigations conducted by contract investigation firms before those investigation reports are provided to customer agencies? What criteria does OPM use to assess the quality and completeness of the investigations during its quality reviews?**

The Office of Personnel Management's (OPM) Federal Investigative Services (FIS) has many levels of quality control throughout our processes to minimize quality concerns with each investigation. Before the Fieldwork Investigative Contractors submit their work to OPM, they are required, under terms of the contract, to perform a quality review of their work. Once a case is submitted to FIS, it goes through FIS' federally controlled review process. At the time of the October 31, 2013 hearing, the review would have been accomplished either by a Federal employee or by an OPM contract employee, depending on case type, complexity, and the issues in the case. However, this arrangement has recently been changed by Director Archuleta. Beginning February 24, 2014, reviews after delivery to OPM are conducted exclusively by Federal employees. Quality inspections are performed to ensure that review was conducted in accordance with the terms of the contract. Once the case is delivered to the agency for adjudication, the agency can return the case to FIS to be reopened if the case does not meet the standards, or they can request that OPM perform additional work outside of the standards.

OPM investigators, whether Federal or contract employees, conduct investigations in accordance with established investigative standards, and OPM has a multi-layered review process to ensure that its investigations make all reasonable attempts to satisfy those standards. To ensure that elements of the investigation within OPM's control are conducted, and that reasonable attempts have been made to obtain those elements that rely on the cooperation and availability of sources, OPM utilizes a number of tools throughout the investigative process so that the ultimate report is as complete as possible. These include an internal Quality Assessment Tool which measures investigations against investigative standards and ensures all adjudicative criteria are properly covered as they are collected, and a random auditing of closed investigations to measure the extent to which the investigations met investigative standards and deliver feedback directly to reviewers' supervisors as well as to FIS' Customer Interface to determine if reopening the investigation for rework is warranted. See FIS's Annual Stakeholder Report for Fiscal Year

2012, pages 14-15 "Delivering Quality," for a further discussion of how FIS conducts quality assessment of its investigative products and processes.

Because source participation during a background investigation is voluntary, at times background investigations will not be complete if personnel are not available for interview, if members of the public are unwilling to provide interviews to investigators, or if records are not made available. In those situations, OPM makes its best effort to locate relevant information through alternative means, and provide notations concerning what is missing.

As with all of its contracts, OPM requires contractors to meet the standards set forth in OPM's contracts. In the case of the investigative fieldwork contracts, as with other Federal contracts, those standards include a requirement that the contractor perform a quality review of all products prior to submitting the finalized product to OPM. In the fieldwork context, this quality review not only helps to support the quality of the final investigative product or service, it also helps to ensure that the quality service or product is delivered on time. A problem that is not addressed until after the report reaches OPM may delay delivery of the final product or service to the requesting agency. And OPM does not need to address quality issues if the contractor addresses them in the first instance, as part of its own performance.

OPM conducts oversight to ensure the quality review requirement is being met, including:

- Review of contract plans that are required to be submitted on an annual basis, including Quality Control and Training plans
- Observations of contractor performance
- Receipt, review, and delivery of Federal feedback in relation to contract requirements
- Weekly evaluations of performance which feed into overall quarterly performance
- Inspections of contractually required investigator evaluation programs, including "check rides" and observance of investigators during the investigation process
- Quarterly inspections of fieldwork contractors regarding quality trending, contractor review output, coverage trending, and contract compliance
- Audits and inspections of the various contracts

FIS' multi layered quality process utilizes a model of continuous improvement across all aspects of our operations, including participation in developing and refining definitive Federal investigative and quality ***standards***; strengthening technology; enhancing training; and refining the Quality Review Process itself. With respect to participation in standards, the Director of National Intelligence and the Director of OPM have jointly issued Federal Investigative Standards to ensure that investigative service providers that perform investigations either for positions that are national security sensitive (including positions that require access to classified information), or investigations required to adjudicate suitability for employment in the Federal competitive or senior executive service are performed to uniform standards for each investigative product used. OPM has also participted in the Data Standards Working Group led by the Office of the Director of National Intelligence (ODNI) which is developing draft standards for Electronic Investigative Reports. OPM, ODNI, and the Department of Defense are co-chairs of the Quality Assessment Working Group which is developing draft standards and a tool intended to measure the quality of background investigations across the Federal government, since the

community recognized that investigative quality, as currently evaluated, is highly subjective. A tracking tool for all investigative service providers and adjudicative agencies will be designed once the metrics have been tested and approved.

With respect to ***technology***, OPM has implemented upgrades to our Field Work System that build in quality assurance factors. In the area of ***training***, OPM requires all investigators to be trained by certified Federal instructors using accredited curriculum. OPM approves and audits contractor training to ensure that it meets the same standard. With regard to the ***Quality Review Process***, OPM requires that after the field work portion of the investigation is completed, it is reviewed by a trained analyst to ensure cases meet the national standards for coverage and resolves issues to the greatest extent possible. If any portion of the case is determined to be deficient during this review it is sent back for corrective action. If at any time, the adjudicative facility determines that FIS did not complete the investigation to standards, it can request the case be reopened at no additional charge.

Working to address GAO's recommendations, FIS developed an internal quality assessment tool to track investigative re-work prior to the closing of investigations. We use those metrics to target training opportunities and policy/procedural changes.

FIS has also restructured to ensure that all functions relating to case review and case closing are housed in one division that focuses upon quality oversight of the final product.

2. **As a result of OPM's quality reviews, how many investigations does OPM send back to each of its contract investigation firms for additional work each month, out of what total number reviewed?**

Our workload fluctuates, but we normally receive between 55,000 to 60,000 fieldwork cases completed by contractors a month, and we return an average of 3.3% as not meeting standards, requiring additional work on the part of the contractor.

3. **In light of the False Claims Act lawsuit against USIS, what specific steps is OPM taking to review the integrity of background investigations that have been conducted by USIS or other OPM contractors?**

OPM was notified by the Department of Justice (DOJ) of the allegations regarding fraud on the part of USIS in August 2011 and began taking steps immediately to address the integrity of the process in light of these allegations. OPM's actions to safeguard the process and ensure any dumping did not continue have included the following:

- Required USIS to remove from the contract 15 USIS officials apparently involved with the misconduct. These individuals are no longer USIS employees.
- Dedicated FIS staff to assist the OIG investigation undertaken as a result of the False Claims Act lawsuit.
- Significantly increased the number of Federal employees performing contractor oversight by a combination of increasing the FTE levels and realigning existing internal staff. Placed a focus on examining the critical USIS processes.

- Commenced the process of recompeting parts of the current Support Services contract to companies who do not possess a fieldwork background investigation contract as an additional step to preclude any conflicts of interest when an OPM contractor reviews an investigative file forwarded to OPM.
- Developed a new tool to detect instances where quality review may not have been performed according to the terms of the contract. Conducted inspections on the average number of reports being reviewed and released by the contractor's review staff for a trend analysis to identify potential concerns.
- Increased the on-site inspections with the contractors' reviews including a comparison of their processes to the technical proposal requirements.
- Increased the frequency of audits of cases closed.

4. **Your testimony, you indicated that OPM has implemented new quality control measures and have an aggressive program to hold investigators to the highest standards of integrity. Please provide the Committee more detail on what these measures are, and how they are enforced.**

Please see the response to Question 1.

5. **What do you see as remaining barriers to agencies providing reciprocity to security clearances granted by other agencies?**

Pursuant to Executive Order 12968 and the Federal Investigative Standards, security clearance reciprocity is mandatory when a person has had no extended break in access," and the employing agency has no indication that unfavorable information has developed since the previous clearance was granted. The Director of National Intelligence, as the Security Executive Agent, has oversight of the application of the reciprocity rules, and is in the best position to respond definitively.

**Post-Hearing Questions for the Record**
**Submitted to Hon. Elaine Kaplan**
**From Senator Tom Coburn**

**"The Navy Yard Tragedy: Examining Government Clearances and Background Checks Hearing"**
**October 31, 2013**

1. **In June, the Subcommittee on Financial and Contracting Oversight held a hearing; "Safeguarding our Nation's Secrets: Examining the Security Clearance Process," where the Inspector General highlighted concerns of lack of adequate Suspension and Debarment authority for security clearance processing. What is the current status of OPM's Suspension and Debarment Program? Are there authorities in place that provides OPM adequate Suspension and Debarment authority?**

Yes. OPM has procedures in place that provide an adequate Suspension and Debarment process, including a Committee and an appointed Suspension and Debarment Official.

Prior to March 21, 2013, OPM presented matters to the Senior Procurement Executive who conducted reviews and determined whether to forward actions to the head of the agency based on circumstances to address contractors who were found to be guilty of violations subject to debarment. On March 21, 2013, a more formal OPM Suspension and Debarment Program wasfully implemented, following the required Federal Register notification period.

OPM also has a separate Suspension and Debarment Program that covers providers under the Federal Employees Health Benefits Program that is administered under its own authority, procedures, and Suspension and Debarment Official.

2. **Recently the Department of Justice intervened in a "qui tam" lawsuit against USIS, it is alleged that USIS violated the False Claims Act by certifying that it conducted reviews of background investigation reports of investigation when in fact it did not. Knowing that this contractor has completed a significant majority of OPM's background investigations is there a plan to evaluate the USIS background investigation product to determine if their services provide the best protection for the American people, classified material and secure facilities?**

OPM was notified by DOJ of the allegations regarding fraud on the part of USIS in August 2011 and began taking steps immediately to address the integrity of the process in light of these allegations. OPM's actions to safeguard the process and ensure any dumping did not continue included the following:

- Required USIS to remove from the contract 15 USIS officials apparently involved with the misconduct. These individuals are no longer USIS employees.
- Dedicated FIS staff to assist the OIG investigation undertaken as a result of the False Claims Act lawsuit.

- Significantly increased the number of Federal employees performing contractor oversight by a combination of increasing the FTE levels and realigning existing internal staff. Placed a focus on examining the critical USIS processes.
- Commenced the process of recompeting parts of the current Support Services contract to companies who do not possess a fieldwork background investigation contract as an additional step to preclude any conflicts of interest when an OPM contractor reviews an investigative file forwarded to OPM.
- Developed a new report to detect instances where quality review may not have been performed according to the terms of the contract. Conducted inspections on the average number of reports being reviewed and released by the contractor's review staff for a trend analysis to identify potential concerns.
- Increased the on-site inspections with the contractors' reviews including a comparison of their processes to the technical proposal requirements.
- Increased the frequency of audits of cases closed by the contractor.

3. **Thank you for the clarification to your response regarding the quality reviews of investigations performed by OPM contractors. Can you provide details of the services provided by the existing OPM contract executed for background investigations with USIS? Can you provide details of the services provided by the existing OPM contract executed for supply services with USIS? Are background investigations for the purpose of Security Clearance or Suitability Determination an inherently governmental function?**

The Office of Management and Budget, which is responsible for guidance concerning what is inherently governmental, has previously determined that, although adjudicating eligibility for access to classified information is an inherently governmental activity, conducting the background investigations that provide the basis for the adjudications is not. GAO also analyzed this issue and agreed that the investigative functions are not inherently governmental.

Regarding the details of the services provided by the existing OPM background investigations contracts, the Fieldwork Contractors, including USIS, conduct investigative fieldwork directly related to a Federal background investigation, which is defined in this context as having four major components: 1) receipt, screening, data entry, case file maintenance 2) conducting investigative fieldwork 3) case review/closing, and 4) post-closing support. It is difficult to be more specific in the context of a document that may become a part of the public record, because it is important that OPM maintain the confidentiality of investigatory processes, so as to perpetuate their usefulness, but, in general, the fieldwork contracts encompass only component 2, conducting investigative fieldwork.

All investigative products/services provided must be in accordance with established Federal investigative standards and the current Investigator's Handbook issued to fieldwork investigators by OPM. Field investigations include work such as conducting Enhanced Subject Interviews (ESI), obtaining personal testimony from a variety of source types, conducting record searches, and reporting all information obtained. Specific work requirements include case

control/assignment, performance to investigative scope and coverage, reports of investigation, management of inventory, and quality control of deliverables to ensure quality standards are met.

Regarding the details of the services provided by the existing OPM contract executed for supply services with USIS the current Support Services contractor, USIS, is assigned support services such as clerical, technical, and analytical personnel. The Support Services components include Switchboard, Screening / Scheduling of Investigative Materials, Case File Maintenance, Imaging / Microfilm, Pre-Review, Case Closings, Mailroom, Telephone Liaison with Agency, and File Release.

4. **OPM's Revolving Fund totals approximately $2 billion annually, and slightly more than half of that is used to fund the Federal Investigative Services. In June, the Inspector General noted that this account had never been audited. Will you provide the status of the any audits conducted on this account? Will an audit be scheduled on a periodic timeframe in the future?**

We are not entirely certain how the Inspector General was using the term "audit" in that testimony. We understand that the auditors of OPM's financial statements, KPMG, routinely do not audit the Revolving Fund in performing the financial statement audits required by the Chief Financial Officers Act. On the other hand, the Office of the Inspector General currently indicates, on its Web page, that its Office of Audits conducts "[a]udits of OPM programs that involve the range of the aegncy's responsibilities, including revolving fund activities such as background investigations and human resources services." See http://www.opm.gov/our-inspector-general/audits/.

OPM has supported the Inspector General's efforts to obtain permission to use funds from the Revolving Fund to finance his activities with respect to the Revolving Fund. And the President's FY2014 Budget included a proposal to permit OPM's Office of the Inspector General (OIG) to access the Revolving Fund for its estimated expenses to adequately audit, investigate, and provide other oversight activities of the Revolving Fund and the activities financed by it. OPM agrees with the importance of strong oversight in order to ensure the integrity of the Revolving Fund, and we look forward to continuing to work with our OIG toward this end.

**Hearing Date: October 31, 2013**
**Committee: SHSGAC**
**Member: Thomas R. Carper, Chairman**
**Witness: Brian Prioletti**

**Question 1: In light of the recent tragedy at the Navy Yard, and the concerns that have been raised about whether Mr. Alexis's clearance should have been revoked, there has been a lot of discussion about when a personnel security clearance should be revoked.**

a. **What types of information regarding current holders of security clearances typically get reported to the security office to investigate, and what are the sources of this information? What actions are typically taken in response to that adverse information?**

**Answer:** Under Executive Orders (EOs) 12968 and EO 10450, each department or agency head has the responsibility to operate and manage an effective personnel security program. Specific organizational constructs and operating guidance in administrating such a program are, therefore unique to each entity. In general, however, any information that has a nexus to the adjudicative guidelines is reportable to the security office by the individual holding the access, and by his or her supervisor(s) and co-workers. This self- and peer-reporting is a core element of the Insider Threat Program. Security professionals within the department or agency then follow their organization's policy and protocols in assessing information received and make appropriate referrals.

b. **If an existing clearance holder is under investigation due to recent discovery of adverse information, to what extent would that adverse information be shared with other executive branch agencies in the event that the person left his or her position before his or her clearance was actually revoked, and then tried to get a position with another agency using clearance reciprocity?**

**Answer:** When an individual under investigation leaves a position requiring access to classified information prior to resolution of the concerns, access to classified information is terminated and the agency sponsoring the individual's clearance provides the termination information and an exception code to Scattered Castles, the Intelligence Community's personnel security repository. This repository currently contains information from the Department of Defense Joint Personnel Adjudication System (JPAS). The Office of the Director of National Intelligence (ODNI) is exploring viable solutions to include security clearance data from the Office of Personnel Management (OPM) Central Verification System (CVS). The recording of an exception code alerts potential gaining agencies of unresolved issues that must be further evaluated before reciprocal acceptance of the security clearance can take place. An exception precludes reciprocity without review of the case by the gaining organization. When discovering an exception code in Scattered Castles, the gaining agency is responsible for contacting the agency providing the exception code for information that resulted in the posting.

Agencies typically update Scattered Castles after completion of an investigation and adjudication or after receipt of unfavorable information that is sufficiently significant to merit the suspension of access; however, an agency may post an exception code to Scattered Castles when

**Hearing Date: October 31, 2013**
**Committee: SHSGAC**
**Member: Thomas R. Carper, Chairman**
**Witness: Brian Prioletti**

information of sufficient concern is raised but that information does not rise to a level which warrants a suspension or revocation. The ODNI recently updated Scattered Castles to bridge gaps that may occur when an individual under investigation changes employers but was not suspended and the allegations did not justify entering an exception code to Scattered Castles prior to the change of employment. Previously, the individual's security clearance would be reciprocally accepted as Scattered Castles would not reflect an exception and the gaining agency was not notified by Scattered Castles that an exception code had been placed upon the individual's termination from the losing agency. To close this gap, Scattered Castles now publishes a daily list of newly issued exception codes, accessible to each agency, which informs agency Scattered Castles Access Managers when a new exception on any individual holding a security clearance with their agency is posted to Scattered Castles. This exception code alerts agencies that have reciprocally accepted a security clearance determination to request information from the agency posting the exception code and to reevaluate the individual.

**Are there any mechanisms in place to facilitate information sharing among agencies about recently discovered adverse information that has not yet led to the revocation of a security clearance, but could negatively affect a person's eligibility to hold a security clearance?**

**Answer**: Ultimately, agencies are responsible for individuals under their cognizance and should notify any other agencies granting the individual access of derogatory information. In addition to manual notification, there are mechanisms in place to notify other agencies intending to reciprocally accept a clearance of adverse information. If information rises to the level that requires an agency to take immediate action to suspend a clearance pending additional investigative efforts, the agency should document the suspension in the appropriate security clearance repository in order to make this information available to other agencies.

In addition, agencies are continuing to expand their reporting of clearance information to multiple repositories (JPAS, CVS, and Scattered Castles), improving information sharing capabilities (i.e., reciprocity) across the entire executive branch. If new adverse information is discovered on an individual possessing a security clearance, agencies post an eligibility exception designation of a Condition, Deviation, or Waiver to the subject's clearance record. This alerts other interested agencies that they should contact the agency holding that information and review the detailed information before granting clearance reciprocity. Scattered Castles publishes a daily listing identifying all newly issued Conditions, Deviations, or Waivers for consideration by adjudicators at each agency.

**Hearing Date: October 31, 2013**
**Committee: SHSGAC**
**Member: Thomas R. Carper, Chairman**
**Witness: Brian Prioletti**

**Question 2: Please clarify when, if ever, random background investigations are conducted before the initial term of a security clearance expires?**

**Answer:** EOs 12968 and 10450, as amended, make department and agency heads responsible for establishing and maintaining an effective personnel security program. In addition to event-driven reinvestigations resulting from concerns regarding an individual's eligibility, agencies may employ random or periodic reinvestigations as part of their personnel security program.

**Question 3: What do you see as remaining barriers to agencies providing reciprocity to security clearances granted by other agencies?**

**Answer**: There are two commonly expressed concerns: first, there are questions regarding the quality or comprehensiveness of an investigation or adjudication being considered for reciprocity; and second, there are questions regarding the application of suitability concerns specific to the receiving agency. The ODNI is currently conducting a reciprocity study to examine reciprocity across the executive branch with the goal of promulgating a policy to provide clear guidance to agencies on the application of reciprocity for security clearances. Reciprocity for employment suitability is regulated by the Office of Personnel Management for those populations covered by OPM's regulations.

**Question 4: With the potential for sequestration reductions to take effect in Fiscal Year 2014, will or has ODNI provide(d) community-wide policy regarding suspension of or delaying reinvestigations for any clearances? If a policy has been issued on this topic, please provide it as an attachment for the record.**

**Answer**: Executive Order 13467 designated the Director of National Intelligence, as the Security Executive Agent (SecEA) and on October 31, 2013, the SecEA, issued guidance to the Executive Branch, acknowledging the fiscal impact of budget shortfalls and sequestration and requiring departments and agencies to use a risk-based approach to prioritize submission of reinvestigations focusing on the highest risk population. The memo identified specific criteria to be considered when prioritizing the population to be reinvestigated. In separate Executive Branch guidance, also issued on October 31, 2013, departments and agencies were directed, by the SecEA, to review and validate their employees' and contractors' need for access to classified information. If eligibility for access to classified information is not required, the departments and agencies were directed to terminate the access, debrief the individual, and annotate the action in the appropriate security clearance repository.

**Hearing Date: October 31, 2013**
**Committee: SHSGAC**
**Member: Thomas R. Carper, Chairman**
**Witness: Brian Prioletti**

**Question 5: To what extent are electronic data, including public and social media, now being used in determining who may be granted or may retain a security clearance, and how do you believe the use of such media and other data could be improved?**

**Answer:** Electronic data is obtained through records checks which are conducted, when possible, against federal, state, and local databases as well as some commercial databases. Information obtained includes criminal records, court records and credit checks. Several agencies are conducting pilot programs on the use of publicly available electronic information/social media to assess the utility of the information available, the resources required to include such checks as part of a security clearance vetting program, filtering of the data and validation of the information, and to identify the measures required to ensure the privacy and civil liberties of the individual.

The use of automated searches and social media enhance an adjudicator's ability to make a well informed eligibility determination. A significant improvement to the personnel security process would be the development of a technical solution that would allow information to be sent automatically or "pushed" to the appropriate agency when a threshold has been met. For example, when an individual is arrested, the arrest information would be "pushed" to the agency holding the individual's security clearance. The concept of "pushing" information is being developed by the ODNI as part of the Continuous Evaluation Program.

**Question 6: How do you believe inherently unreliable electronic data, such as certain social media, can and should be used for determining who may be granted or may retain a security clearance?**

**Answer:** The social media pilot programs conducted to date demonstrate that information potentially relevant to an eligibility determination exists on internet sites. These same pilots have demonstrated a need for information developed from social media sites to be validated rather than accepted as fact. Electronic data is not inherently different from any other data collected during a background investigation. Regardless of the source, noteworthy information must be explored to verify the accuracy of the information, develop details regarding the issue, and identify sources that support or mitigate the issue. In the end, decisions to grant or deny a clearance are not made on unsubstantiated data, but on a compilation of data from multiple sources that present a detailed, "whole person" view of the subject of the investigation.

**Hearing Date: October 31, 2013**
**Committee: SHSGAC**
**Member: Tom Coburn, Ranking Member**
**Witness: Brian Prioletti**

**Question 1: Security clearances are granted on a need-to-know basis when there is a demonstrated need for access to classified information, clearances are required. There are currently more than 5.5 million people with Security Clearances, of those 1.4 million are Top Secret. Has the Office of the Director of National Intelligence conducted a study or review to evaluate the requirements for security clearances? If so, when was this completed and what were the results?**

**Answer:** According to the Director of National Intelligence (DNI's) *2012 Report on Security Clearance Determinations,* as of October 1, 2012, 4.9 million individuals were eligible to hold or held a security clearance. Of those, 1.4 million were eligible or in access at the Top Secret level, and 3.5 million were eligible or in access at the Confidential /Secret level. An alternate way to analyze the 4.9 million figure is to break out those in access versus those who were not in access but were investigated and determined to be eligible for access. Using that analysis, 3.1 million individuals were in access at the Secret and Top Secret levels, while 1.8 million were eligible for access to classified information or to hold a sensitive position. The reporting of "eligibility" provides insight as to the actual number of individuals in access or who *may be* briefed into access on a moment's notice, thereby providing a better understanding of the potential impact on investigative and adjudicative resources. Eligibility reporting may, however, create the perception of a growing number of individuals with a need for access to classified information. The 2013 *Report on Security Clearance Determinations* will include a breakdown of individuals who are eligible for access versus those actually in access.

The DNI, as the Security Executive Agent, issued an executive correspondence, *Validation of Personnel with Eligibility for Access to Classified Information*, on October 31, 2013. This correspondence requires agency heads to validate against the conditions set forth in Executive Order (EO) 12968, as amended, whether or not each individual employee or contractor requires eligibility for access to classified information. The correspondence further requires individuals no longer requiring access to be debriefed and for the debriefings to be recorded in the requisite security repositories. In addition, the Office of the Director of National Intelligence (ODNI) is currently working with the Office of Personnel Management to reissue Title 5 of the Code of Federal Regulations, Office of Personnel, Part 732, National Security Positions (5 CFR 1400) to clarify the requirements and procedures agencies should observe when designating, as national security positions, positions in the competitive service; positions in the excepted service where the incumbent can be noncompetitively converted to the competitive service; and Senior Executive Service positions filled by career appointments. The referenced regulation calls for agencies with these populations to reevaluate their positions against the requirements of the regulation within 24 months of its final issuance. We note that while all positions requiring security clearances are properly designated as national security positions, there are additional categories of positions where the incumbents do not require security clearances, but the positions must nonetheless be designated as national security sensitive pursuant to a presidential executive order (E.O. 10450). The proposed regulations will seek to promote quality and consistency in making position designations for these categories of positions.

**Hearing Date: October 31, 2013**
**Committee: SHSGAC**
**Member: Tom Coburn, Ranking Member**
**Witness: Brian Prioletti**

**Question 2: The Information Security Oversight Office's Report to the President for Fiscal Year 2012 documented a 42% reduction in original classification activity. The number of officials with original classification authority is at its lowest recorded level, down to 2,326 from a high of 7,149 in 1980. What recent management decisions directly impacted this significant decrease?**

**Answer:** The ODNI does not have further insight into the driving forces resulting in a 42% reduction in the number of original classification authorities in the departments and agencies across the government. The Information Security Oversight Office (ISOO) is responsible to the President for policy and oversight of the Government-wide security classification system, and the ODNI respectfully defers to the ISOO on this issue.

**Question 3: How can the Department of Defense and other agencies accurately determine what material should be classified and ensure they are not over-classifying materials? Are we? If so, why? How much of the extensive increase to documents considered classified is linked to government service contracts that contain excessive proprietary information?**

**Answer:** The ISOO is responsible to the President for policy and oversight of the Government-wide security classification system, and departments and agencies are responsible for accurately identifying and marking their own classified information. ODNI respectfully defers to the ISOO and the Department of Defense on this issue.

**Question 4: After Aaron Alexis was discharged from the Navy, The Experts, a Fort Lauderdale-based information technology company that was a subcontractor for Hewlett-Packard on a Navy program requested to transfer his secret clearance to his new position. Can you explain this process and explain why this is an accepted practice by the Department of Defense. Why is this acceptable without a new investigation taking place?**

**Answer:** As the Aaron Alexis case remains an ongoing investigation, this response is limited to the security clearance reciprocity process. Security clearance reciprocity standards are set forth in EOs 12968, as amended, and 13467; various Office of Management and Budget (OMB) memorandums issued in 2005, 2006 and 2007; and Intelligence Community Policy Guidance. Reciprocity guidance for a Secret level clearance is specifically covered under the executive orders and OMB memoranda. The standards for a Secret level clearance permit reciprocal acceptance of a Secret level clearance if the background investigation is less than ten-years old, absent any issues of concern related to the individual's eligibility for access to classified information. Departments and agencies are required to query the requisite security clearance repositories for information of concern prior to reciprocally acceptance of a security clearance.

CHARRTS No.: SHSGAC-05-004
Senate Committee on Governmental Affairs
Hearing Date: October 31, 2013
Subject: The Navy Yard Tragedy: Examining Government Clearances and Background Checks Hearings
Witness: Mr. Lewis
Senator: Senator McCaskill
Question: #1

Question. Which Department of Defense divisions provide individuals temporary access to their facilities prior to completing background checks? For each division that provides temporary assess prior to completing background checks, please provide the following details:

a. What is the process for obtaining temporary access to a facility?

b. What, if any, security checks are performed prior to granting temporary access?

c. When are background checks performed after an individual has been given temporary access?

d. For how long is the temporary access granted?

e. What, if any, access restrictions are in place when an individual has only been granted temporary access?

Answer. Generally, the Departments of the Army, Navy (includes the Marine Corps) and Air Force report that they provide individuals unescorted access only after completing a National Crime Information Center (NCIC) database check, except for special events, circumstances or activities and for emergency operations.

a. Commanders are responsible for maintaining a visitor control program to ensure only authorized individuals enter an installation. Screening/vetting of visitors against the NCIC is available to every installation, but not necessarily at the point of entry. Additionally, security forces verify the identity of personnel entering an installation by visually examining Common Access Cards (CAC), other military ID cards (e.g., those issued to retirees or family members), state/local government issued ID cards (e.g., drivers licenses, etc.), or locally-produced, temporary visitor identification or passes.

b. Except for special events, circumstances or activities and emergency operations, a check of records through the NCIC is required prior to granting unescorted access. Additionally, at Navy bases vendor-users not CAC-eligible use the Navy Commercial Access Control System (NCACS) and receive a check of records through the Sex Offenders Registration and Notification Act database (SORNA), Consolidated Law Enforcement Operations Center system (CLEOC) and Terrorist Screening Database (TSDB) as baseline background checks for entry onto Navy installations prior to being issued Temporary Passes, in accordance with governing documents.

For vendors/contractors who do not wish to enroll in the NCACS program, a NCIC database check is completed before granting temporary access.

For visitors with sponsors, sponsors escort visitors and are responsible for their actions while aboard the installation. Sponsored visitors in most cases do not receive a NCIC check except on a random basis. Non-CAC eligible contractors and vendors are required to conduct background checks on their employees and provide an access control roster to installation commanders prior to beginning work on the installation.
All installations use Random Anti-terrorism Measures (RAM) dependent on manpower and equipment availability to conduct searches for contraband, weapons, etc.

c. This is dependent on the individual's purpose for access, where access is needed, and the amount of time for which access is granted. For example, for short time periods, such as one-day access for families of graduating recruits at the recruit training center and depots, NCIC checks are not completed.

All contractors receive NCIC database check prior to entry onto Navy and Marine Corps installations.

When the Department of Justice/JUST OPENFOX Web-based Program is available at Navy installations, access to NCIC databases will be available at installation Pass and Identification offices and Dispatch Centers. This will provide access to NCIC and other responsive information at the point-of-entry, to include NCIC background checks of all visitors.

d. Dependent on requirement, Commanders will use a locally produced, temporary issue, visitor identification system pass with an expiration date. The expiration date of the pass will be the end date of the contract or visit, or the expiration date of the sponsor's credential, whichever occurs first.

Navy does not allow the pass to exceed 180 days.

For Marine Corps installations, access for sponsored visitors is granted per local policy, and generally allows for time periods requested by the sponsor. Contractors and vendors are granted access per contract language and requirements to complete performance of work.

e. Access control restricts and/or controls entrance to property and/or installations to only those authorized persons and their vehicles. Persons authorized temporary access may be either escorted or unescorted depending on requirements and mitigation efforts in-place. Non-DoD affiliated personnel who do not have an approved official purpose and have not undergone NCIC vetting will generally be escorted while on the installation or access only limited areas.

Additionally, for some installations, restrictions are noted in contract language that specifies vendors and contractors have access only during working hours.

CHARRTS No.: SHSGAC-05-001
Senate Committee on Governmental Affairs
Hearing Date: October 31, 2013
Subject: The Navy Yard Tragedy: Examining Government Clearances and Background Checks Hearings
Witness: Mr. Lewis
Senator: Senator Coburn
Question: #1

Question. In 2008, DoD Changed a Security Clearance Question on Mental Health on Standard Form 86, this due to a perception that "it is needlessly preventing some people from seeking counseling," can you discuss that decision?

a. Have you seen the number of DoD members initiating some sort of mental health counseling increase since this change was made?

b. How should the Department ensure that the mental health of an individual is covered in the investigation process?

Answer. DoD did indeed advocate a change to Question 21 on the Standard Form 86, "Questionnaire for National Security Positions," which relates to mental health counseling. This initiative was prompted by a concern that DoD personnel, who are routinely exposed to traumatic events with psychological impact beyond those encountered in other environments, were not seeking the mental health counseling needed to deal with these experiences. In 2008, the Office of Personnel Management, with the concurrence of the Director of National Intelligence, issued a change to the form which provided an exemption from reporting mental health counseling "..strictly related to adjustments from service in a military combat environment."

a. Unfortunately, we do not have data responsive to the question "Have you seen the number of DOD members initiating some sort of mental health counseling increase since this change was made?"

b. DoD is an active participant in the ongoing Office of Management and Budget (OMB) 120-day Suitability and Security Processes Review which is examining the personnel security process. In accordance with Executive Order 13467, the Director of National Intelligence is the Security Executive Agent responsible for oversight of investigations used to determine eligibility for access to classified information, and the Director of the Office of Personnel Management has a similar responsibility regarding investigations used to make determinations of suitability and eligibility for logical or physical access.

CHARRTS No.: SHSGAC-05-002
Senate Committee on Governmental Affairs
Hearing Date: October 31, 2013
Subject: The Navy Yard Tragedy: Examining Government Clearances and Background Checks Hearings
Witness: Mr. Lewis
Senator: Senator Coburn
Question: #2

Question. How many Security Clearances were denied by the Department of Defense in 2012? How many have been denied in the last five years?

a. Does the adjudication of an individual by its sponsoring agency create a conflict of interest? How much impact does the agency's need to have positions filled, have on the adjudication process?

b. Are there sufficient incentives to say no to a clearance that could pose some risks?

Answer. In 2012, a total of 10,968 adjudications resulted in denial or revocation of a security clearance. Over the last five years, a total of 62,617 adjudications resulted in denial or revocation of a security clearance. Denials and revocations represent approximately 2% of adjudicative determinations.

a. The adjudication of an individual by its sponsoring agency does not create a conflict of interest primarily because DoD has consolidated most of its adjudicative activity in the DoD Consolidated Adjudications Facility (DoD CAF) which operates independently of the DoD components.

The agency's need to have positions filled has little to no impact on the adjudication process. The DoD CAF has established close working relationships with all of its customers. If a customer has a pressing need for the DoD CAF to quickly adjudicate a particular individual's background investigation, the DoD CAF is able to expedite its review of that case by moving the case forward in the queue. This has no impact on the adjudicative outcome; it is simply a matter of prioritizing workloads.

b. There are sufficient incentives to say no to a clearance that could pose risks. The final adjudicative determination has no impact on the individual adjudicator; the adjudicators are neutral as to the outcome of any particular adjudication. The productivity standards that adjudicators operate under are weighted to account for the time required to adjudicate a case to a denial or revocation, so there is no difference to the adjudicator if they grant or deny a clearance. Further, the adjudicators comprise a professional workforce that takes pride in doing their jobs the right way and is subject to independent reviews of its adjudicative decisions. One way to look at it is there is no incentive to simply grant clearances; adjudicators are incentivized to make the proper determination in each case.

CHARRTS No.: SHSGAC-05-003
Senate Committee on Governmental Affairs
Hearing Date: October 31, 2013
Subject: The Navy Yard Tragedy: Examining Government Clearances and Background Checks Hearings
Witness: Mr. Lewis
Senator: Senator Coburn
Question: #3

Question. A recent DoD Inspector General report revealed that 52 convicted felons received routine, unauthorized installation access, placing military personnel, dependents, civilians, and installations at an increased security risk. It was determined that this lapse occurred because the Navy Installations Command did not perform a comprehensive business case analysis and issued policy that prevented transparent cost accounting of Navy Commercial Access Control System. What actions have been done taken to correct this security threat from happening in the future?

Answer. Navy no longer issues temporary passes until a National Crime Information Center (NCIC)/Terrorist Database check is completed. With regard to the 52 felons cited in the DoD IG report, the Navy immediately upon receipt of the names from the DoD IG rescreened all 52. Of those 52, 36 were granted waivers by the applicable installation commander and 16 had their access to the base/installation denied, although it is likely some were issued temporary, 28-day access passes before their waivers were adjudicated.

The Navy's access control process has provisions for an individual who is determined to have a felony conviction to request a waiver from the installation commanding officer (CO). For waivers, the Installation CO makes a risk decision based on the individual's criminal record, where they will be working and what they will be doing on the installation, and what facilities/activities are on the installation.

The Navy Commercial Access Control System (NCACS) is used for those contractor personnel who do NOT meet the criteria for issuance of a DoD Common Access Card (CAC) (i.e., documented requirement for routine access for six months or more). NCACS is used for issuing credentials to allow for installation access to those contractor personnel who require recurring access to a base or installation to deliver goods or provide services (e.g., lawn mowing).

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

December 6, 2013

The Honorable Thomas R. Carper
Chairman
The Honorable Tom A. Coburn
Ranking Member
Committee on Homeland Security and Governmental Affairs
United States Senate

Subject: *GAO Response to Questions for the Record Regarding the Personnel Security Clearances Process*

Thank you for the opportunity to testify before your subcommittees on October 31, 2013, during the hearing, *The Navy Yard Tragedy: Examining Government Clearances and Background Checks*. In the attached enclosure, please see our responses to the Questions for the Record submitted by Ranking Member Coburn. The answers to these questions are based on our reports and testimonies used to develop the statement I provided for the hearing (GAO-14-157T). This work was conducted in accordance with generally accepted government auditing standards. Further details about the scope and methodology can be found in each of the related products of GAO-14-157T.

If you or other members of your subcommittees have any additional questions about the government-wide personnel security clearance process, please contact me on (202) 512-3604 or farrellb@gao.gov.

Brenda S. Farrell

Brenda S. Farrell
Director, Defense Capabilities and Management

Enclosures

**Post-Hearing Questions for the Record**
**Submitted to Ms. Brenda Farrell**
**From Senator Tom Coburn**

**"The Navy Yard Tragedy: Examining Government Clearances and Background Checks Hearing"**
**October 31, 2013**

1. **In your opening statement you mentioned that the executive branch agencies have not fully developed and implemented metrics to measure quality in key aspects of the personnel security clearance process. You specifically mentioned investigative reports and adjudicative files.**
   a. **Does OPM have metrics that measure the completeness of its investigative reports?**

At the time of our 2009 review, we reported that the Office of Personnel Management (OPM) does not measure the extent to which its investigative reports meet federal investigative standards.[1] We reported in 2009 that the only measure of quality that OPM used was the frequency with which adjudicating agencies returned OPM's investigative reports due to deficiencies in quality. Specifically, OPM tracks investigations that are (1) returned for rework from the requesting agency, (2) identified as deficient using a web-based customer satisfaction survey, or (3) identified as deficient through adjudicator calls to OPM's quality hotline. However, we noted in our 2009 report that the number of investigations returned for rework is not by itself a valid indicator of the quality of investigative work because both Department of Defense (DOD) leadership and adjudicators told us that they have been reluctant to return incomplete investigative reports because of their perception that returning the reports would result in delays in the clearance process. Further, relying on agencies to voluntarily provide information on investigation quality may not reflect the quality of OPM's total investigation workload.

In February 2011, we reported that the leaders of the joint reform effort—Office of Management and Budget (OMB), Office of the Director of National Intelligence (ODNI), OPM, and DOD—under the Performance Accountability Council engaged in an effort in March 2010 to develop quality metrics for security clearance investigations and adjudications.[2] In May 2010, the leaders of the reform effort provided the Subcommittee on Oversight of Government Management, the Federal Workforce, and the District of Columbia, Committee on Homeland Security and Governmental Affairs of the U.S. Senate with 15 metrics to be used to assess the timeliness and quality of investigations, adjudications, reciprocity, and the automation of the personnel security clearance process. We reported that the quality metrics, in turn, could be used to gauge progress

[1] GAO, *DOD Personnel Clearances: Comprehensive Timeliness Reporting, Complete Clearance Documentation, and Quality Measures Are Needed to Further Improve the Clearance Process*, GAO-09-400 (Washington, D.C.: May 19, 2009).

[2] GAO, *High-Risk Series: An Update*, GAO-11-278 (Washington, D.C.: February 2011).

and assess the quality of the personnel security clearance process. We found that these were positive developments that could contribute to greater visibility over the clearance process, including the quality of investigations and adjudications. However, these performance measures have not been fully implemented. For example, the Rapid Assessment of Incomplete Security Evaluations was one tool the executive branch agencies planned to use for measuring quality, or completeness, of OPM's background investigations. In June 2012, an OPM official stated that OPM chose not to use this tool and opted to develop another tool. In following up on our 2009 recommendations, in August 2013 OPM provided GAO with information on its Review Quality Tool that it stated OPM is using to review investigations against investigative standards. However, at that time, OPM had not provided enough details on its tool for us to determine if the tool met the intent of our 2009 recommendation, and included the attributes of successful performance measures identified in best practices, nor could we determine the extent to which the tool was being used.

**b. Did they provide an explanation for any reports that were submitted to the respective agency incomplete?**

We reported in 2009 that officials in OPM's Federal Investigative Services Division stated that gathering all of the information required by the federal investigative standards does not necessarily indicate a quality investigation.[3] OPM officials also stated that an investigative report that includes all of the items required by the federal investigative standards does not equate to having obtained the right or best sources of information about an applicant. Further, officials from OPM's Federal Investigative Services Division's Quality Management and Training Group reviewed eight of the investigative reports we reviewed for our 2009 report and agreed with some but not all of the items we had identified as missing in the reports. Nonetheless, OPM officials concurred with our assessment that documentation for at least one item required by federal investigative standards or OPM's internal guidance was missing in each of the eight investigative reports.

In addition, we reported in 2009 that while OPM does not assess its reports for completeness, it does conduct report reviews that make judgments of, among other things, whether an investigative report is sufficient to enable an adjudicator to make a clearance decision. When making judgments, we reported in 2009 that OPM report reviewers consider the federal investigative standards as well as the unique aspects of each investigation. For example, federal investigative standards require an interview of the applicant, and OPM report reviewers consider whether an applicant is available for that interview in instances in which that applicant is deployed to a remote location. While OPM reviews its own investigative reports, these reviews are not data-driven

[3]In our 2009 report, when discussing the incomplete documentation in OPM's investigative files, we explained that we did not make evaluative judgments about the importance of one missing investigative item over another during our review because the federal investigative standards do not assign a level of importance to each investigative requirement.

measures of the frequency with which investigative reports meet federal investigative standards. By not measuring the completeness of investigative reports using the federal investigative standards, OPM is limited in its ability to explain the extent to which incomplete reports exist and reasons why some reports are incomplete.

**2. In your work with the security clearance process resulted in any dissatisfaction with the OPM investigative reports from DOD or other agency officials?**

**a. Have any agency officials who utilize OPM as their investigative service provider, cited challenges related to deficient investigative reports?**

Our November 2010 report discussed several challenges that agencies faced in meeting the timeliness objectives in the Intelligence Reform and Terrorism Prevention Act of 2004,[4] and these challenges included investigation services quality and cost. Specifically, we reported that officials representing the Departments of Homeland Security, Energy, the Treasury, Justice, and four DOD component agencies[5] that utilize OPM as their investigative service provider cited challenges related to deficient investigative reports as a factor that slows agencies' abilities to make adjudicative decisions.[6] We also reported in 2010 that several agency officials stated that in order to avoid further costs or delays they often choose to perform additional steps internally to obtain missing information, clarify or explain issues identified in investigative reports, or gather evidence for issue resolution or mitigation. Further, we noted in our 2009 report that incomplete investigative documentation may lead to increases in the time it takes to complete the clearance process and the overall costs of the process.[7] Our 2009 report also stated that incomplete documentation in the clearance process may reduce the assurance that appropriate safeguards are in place to prevent clearances from being granted to untrustworthy individuals.

[4]Pub. L. No. 108-458, §3001 (2004) (codified at 50 U.S.C. § 3341). While IRTPA was a far-reaching act with many broad implications, our references to it in these responses pertain solely to section 3001.

[5]These DOD component agencies include the Joint Chiefs of Staff, Army, Navy, and the Defense Office of Hearings and Appeals. The Defense Intelligence Agency, who adjudicates certain cases for the Joint Chiefs of Staff and Washington Headquarters Services, provided similar comments.

[6]GAO, *Personnel Security Clearances: Pragress Has Been Made to Improve Timeliness but Continued Oversight Is Needed to Sustain Momentum*, GAO-11-65 (Washington, D.C.: Nov. 19, 2010).

[7]GAO-09-400.

**b. What impact have deficient reports had on the agencies' abilities to make adjudicative decisions?**

In our May 2009 report, we found that incomplete OPM-provided investigative reports negatively affect the clearance process, leading to delays and increasing the cost of DOD's personnel security clearance process.[8] We also reported in 2009 that DOD adjudication facility leadership told us that at times they perform limited investigative work—such as obtaining bankruptcy records—to comply with investigative standards to fill the gaps in information they have received. Conducting investigative work at this point in the process increases the amount of time and labor costs required to make an adjudicative determination. Further, incomplete adjudication documentation may introduce risk in the clearance renewal phase of the clearance process. In 2009, we reported that some DOD adjudicators and adjudication facility leadership raised concerns that incomplete initial adjudicative files can negatively affect their ability to identify trends when they adjudicate clearance renewals. Similarly, in November 2010, we reported that deficiencies in investigative reports affect the quality and timeliness of the adjudicative process.[9] Specifically, we reported that agency officials who utilize OPM as their investigative service provider cited challenges related to deficient investigative reports as a factor that slows agencies' abilities to make adjudicative decisions. We reported in 2010 that the quality and completeness of investigative reports directly affects adjudicator workloads, including whether additional steps are required before adjudications can be made, as well as agency costs.

**c. Have any agency officials who utilize OPM as their investigative service provider, cited OPM investigative reports that did not include associated police reports and criminal record checks for individuals being investigated?**

In November 2010, we reported that some agency officials noted that OPM investigative reports do not include complete copies of associated police reports and criminal record checks.[10] As we reported in 2010, ODNI and OPM officials told us that OPM investigators provided a summary of police and criminal reports, and asserted that there is no policy requiring inclusion of copies of the original records. However, ODNI officials also stated that adjudicators may want or need entire records as critical elements may be left out of the investigator's summary. For example, according to Defense Office of Hearings and Appeals officials, in one case, an investigator's summary of a police report incorrectly identified the subject as a thief when the subject was actually the victim. If the Defense Office of Hearings and Appeals had access to actual police documents, officials believe the adjudication process would be more efficient.

---

[8]GAO-09-400.

[9]GAO-11-65.

[10]GAO-11-65.

3. **In 2009, you made two recommendations to improve the quality of adjudicative files for DOD. First, that DOD measures the frequency with which adjudicative files meet requirements. Second, that DOD issue guidance to clarify when adjudicators may use incomplete investigative reports as the basis for granting clearances. In response to your recommendation, DOD established RADAR, guidance that outlines the minimum documentation requirements adjudicators must adhere to when documenting security clearance determinations and provides standards to be used for the sufficient explanation of incomplete investigative reports. How have these actions taken by DOD improved the current security clearance process?**

GAO has not independently assessed the extent that DOD's Review of Adjudication Documentation Accuracy and Rationales (RADAR) tool has improved the current security clearance process; however, in following up on the status of our 2009 recommendations, as of 2012, a DOD official stated that RADAR had been used in fiscal year 2010 to evaluate some adjudications, but was not used in fiscal year 2011 due to funding shortfalls. DOD stated that it restarted the use of RADAR in fiscal year 2012. In June 2013, DOD officials told us that the use of RADAR assessments indicated that vast majority of cases met the standards for adjudication documentation and consistency with national adjudication standards in 2010, and that preliminary results showed that this rate increased even more in 2012. In addition, these officials identified several actions DOD has taken to focus on quality on the adjudicative process. For example, DOD officials told us that they have an internal quality assessment team that conducts independent quality reviews and maintains quality metrics and assessments, and that supervisors conduct random quality reviews. GAO has not independently evaluated the accuracy of DOD's stated rates for cases meeting adjudication documentation standards or the extent to which the other actions taken may have improved the security clearance process. However, we are beginning work to further review the quality of security clearance background investigations.

# THE NAVY YARD TRAGEDY: EXAMINING PHYSICAL SECURITY FOR FEDERAL FACILITIES

**TUESDAY, DECEMBER 17, 2013**

U.S. SENATE,
COMMITTEE ON HOMELAND SECURITY
AND GOVERNMENTAL AFFAIRS,
*Washington, DC.*

The Committee met, pursuant to notice, at 10:34 a.m., in room SD–342, Dirksen Senate Office Building, Hon. Thomas R. Carper, Chairman of the Committee, presiding.

Present: Senators Carper, Heitkamp, Coburn, and Ayotte.

## OPENING STATEMENT OF CHAIRMAN CARPER

Chairman CARPER. Good morning, Senator Heitkamp. The early bird.

Senator HEITKAMP. Good morning, Mr. Chairman.

Chairman CARPER. How are you doing? You sound in good voice today.

Welcome, everyone. Thank you for joining us, and some of you, thank you for joining us again and again. It is nice to see you all.

This is an important hearing. This is actually the second in a series of hearings that will enable us to take a closer look at physical security for Federal facilities.

Three months ago, as we know, Aaron Alexis reported to the Washington Navy Yard with intentions to inflict pain and suffering on anyone in his path. We do not know now and maybe we never will be entirely clear why this tragedy came to pass, but hopefully the lessons learned from it will provide a foundation for preventing future tragedies like this one.

Let us take just a moment to recount how Aaron Alexis got the access to the Navy Yard that allowed him to successfully enter the facility that fateful morning.

In 2007, Aaron Alexis joined the U.S. Navy. As with other servicemembers, a background check was performed and he was granted a low-level security clearance. After an honorable discharge from the Navy in 2011, Alexis was hired by a defense contractor who confirmed that he possessed a valid security clearance.

This marked him as a trustworthy individual. Because of that security clearance and that job, Alexis was provided with an ID card that would authorize his access to certain facilities, including Building 197 at the Washington Navy Yard.

Shortly before 8 a.m., on September 16, 2013, Aaron Alexis drove to the front gate of the Washington Navy Yard and displayed his

access card. He was admitted by security, parked his car, and walked to Building 197.

Upon entering that building, Alexis encountered two additional security layers: an automated turnstile which required a valid access card and an armed security guard posted near an entrance.

Unfortunately, these measures were designed primarily to prevent unauthorized access and not to screen for weapons. Officials probably thought that the people working there were trustworthy because they had security clearances and had been vetted.

Eight minutes after Alexis cleared security, he began shooting coworkers using a shotgun that he had successfully concealed.

In the wake of the shooting at the Washington Navy Yard, this Committee began a review of security practices and procedures highlighted by the attack.

Our first oversight hearing looked at the security clearance processes that Federal agencies have implemented to determine who should have access to sensitive information or to facilities. At that hearing we explored ways to improve the process and were reminded that quality cannot be sacrificed for speed. The purpose of today's hearing is to review how we physically secure Federal facilities from attack.

In many instances, security measures begin long before a person approaches the facility. Because Mr. Alexis was able to maintain a security clearance, he was trusted as a defense contractor and granted access to the Navy Yard complex. Aaron Alexis exploited this trust, and he hurt a lot of innocent people.

In the aftermath, it is only natural that we wonder if all people entering a Federal facility—even employees—should be screened in some way. Should we, to borrow an often used phrase from Ronald Reagan, "trust, but verify"?

Workplace violence and insider threats are just some of the examples of the many undesirable threats facing our Federal facilities. There are many other potential threats that agencies must attempt to detect and deter. In addition to active shooters, agencies must develop countermeasures for improved explosive devices, biological weapons, and other types of assaults.

Today's hearing will examine Federal agencies' efforts to develop and maintain effective layers of security at their facilities and prevent future attacks against innocent people.

Facility security is not just about protecting the physical structure of a building; it is about safeguarding the millions of innocent people who work and visit these facilities on an almost daily basis. Today's hearing on facility security is also about honoring the memory of the 12 men and women who died on September 16, earlier this year by learning from that incident and doing all that we can to prevent a similar tragedy from happening in the future.

People who work with me know that one of my guiding principles is, "If it is not perfect, make it better." And our goal today is to figure out how we can do a better job protecting people at our Federal facilities. We can start by asking some fundamental questions.

First, we need to ask: How do Federal agencies determine what the threats are to their specific facilities?

As we know, not every facility is the same. Large Federal buildings in big cities—for example, the Alfred P. Murrah building in

Oklahoma City—may be a target for terrorists because of their size and what they symbolize. However, the more likely threat is probably to a small Social Security office or maybe an Internal Revenue Service (IRS) Taxpayer Assistance Center because of a tired or angry citizen reacting badly and out of impulse.

Second, we should ask: Are Federal agencies properly assessing and prioritizing these risks?

As we all know, the world around us is constantly changing. So is the nature of the threats that we face. As a result, methods for securing our homeland should always be under observation and under assessment because the nature of the threat continues to evolve. The methods we use to secure our homeland must continue to evolve.

That leads me to my final question, and that is: How do agencies respond to these evolving threats?

A security measure that may work for one facility may not work for another. For example, not every facility might be able to be built 50 feet or more away from the nearest public road in order to protect against a vehicle-borne threat.

I also want to know if Federal agencies are sufficiently sharing best practices. Is the Department of Defense (DOD) working with civilian agencies to share its expertise and its experience?

For both military and civilian facilities, senior officials at a facility are responsible for determining which security measures should be implemented. However, civilian officials sitting on a local Facility Security Committee (FSC) may have little or no training in security matters; whereas, the commanding officer for a military installation may have years of experience and education in security matters.

Most importantly, I want to know what actions different organizations have undertaken since the Navy Yard shooting to improve security at Federal facilities.

Many departments and agencies bear some responsibility for securing Federal facilities. This includes the Department of Defense and the General Services Administration (GSA) and even the Department of Energy (DOE). It also includes the Federal Protective Service (FPS), a component of the Department of Homeland Security (DHS) that is responsible for protecting Federal facilities owned or leased by the General Services Administration.

There is no doubt that the Federal Protective Service has a difficult mission. That agency employs only about 1,000 law enforcement officers to protect more than 9,000 civilian Federal facilities. Think about that. These facilities are spread out all across the country.

Yet while the Federal Protective Service is responsible for assessing security at each of these facilities, it lacks complete authority to implement security measures. It may recommend installing metal detectors and X-ray screening equipment at a facility, but it is the local Facility Security Committee that decides whether to authorize and pay for those recommended security measures.

As repeated Government Accountability Office (GAO) reports have highlighted, a number of internal management challenges have impeded the Federal Protective Service's ability to protect facilities. For example, the Federal Protective Service must complete

the facility security assessments in a timely manner so that it can share them with the offices it protects. Because the Federal Protective Service has been unable to do that, other agencies have sought to complete their own facility security assessments, creating unnecessary duplication and waste.

The Federal Protective Service must also do a better job of tracking and overseeing training for the 14,000 contract guards that it uses to protect facilities. The agency must ensure both its Federal law enforcement officers and the armed security guards it uses are appropriately trained, equipped, and prepared.

Ensuring the training, the equipment, and the preparedness of Federal law enforcement officers and armed contract security guards is central to providing for the security of the facilities safeguarded by the Federal Protective Service. This will require, at a minimum, a greater focus on active-shooter scenario training. In the wake of the shootings at the Navy Yard and the Wheeling, West Virginia, Courthouse, we cannot afford to be ill prepared for this type of threat.

While Director Eric Patterson has worked hard to improve the Federal Protective Service's performance, the agency has not always received the support it needs from Congress. I want to assure Director Patterson that I am committed to working with him to make the agency more efficient and more effective. We can start by focusing on the cost-saving or cost-neutral solutions that are much more likely to receive broad bipartisan support from our colleagues here in Congress.

I hope that today's hearing will help us find better ways to improve security at all Federal facilities. I believe there is much to be learned from the Navy Yard tragedy to help us prevent similar incidents in the future.

And I suspect we will be joined here later this morning by Dr. Coburn, who I know has a strong interest in these issues.

Normally I do not turn to the Senator from North Dakota to see if she would like to make a comment or two, but you are welcome to, if you would like, Heidi.

Senator HEITKAMP. No. Mr. Chairman, we will go ahead and proceed.

Chairman CARPER. OK. I am going to just briefly introduce our witnesses and reintroduce others.

I want to introduce as our first witness Caitlin—do you pronounce your name "Durkovich"?

Ms. DURKOVICH. Yes.

Chairman CARPER. Caitlin Durkovich, Assistant Secretary for Infrastructure Protection for the National Protection and Programs Directorate (NPPD) at the Department of Homeland Security, where we have a newly confirmed Secretary, Jeh Johnson, who was approved I think yesterday by a vote of about 78–16. I just would say here publicly how grateful I am to our colleagues, Democrat and Republican, for their support, especially to Dr. Coburn, who was a strong supporter of Jeh's nomination. And I think it may take a couple of days to process the paperwork so that he can be sworn in and be on the payroll, but we need him in place, and he needs a team to lead, including an able Deputy Secretary of Home-

land Security. I believe Alejandro Mayorkas, if confirmed, will be that person.

Ms. Durkovich was appointed to her current position in May 2012. As Assistant Secretary for Infrastructure Protection, Ms. Durkovich leads the Department's efforts to strengthen and build resilience in our Nation's critical infrastructure. As Chair of the Interagency Security Committee (ISC), Ms. Durkovich oversees its mission to develop security standards and best practices for civilian Federal facilities in the United States.

Our next witness is Retired Brigadier General Eric Patterson—great to see you—Director of the Federal Protective Service, a component of the Department of Homeland Security's National Protection and Programs Directorate. Director Patterson was appointed to his position in September 2010. As Director, Mr. Patterson oversees the Service's mission to protect and deliver integrated law enforcement and security services to over 9,000 civilian Federal facilities and to safeguard their more than 1.4 million daily occupants and visitors.

Now, I understand you served in the Air Force for over 30 years.

General PATTERSON. Yes, sir.

Chairman CARPER. Thank you for that service, too.

Our final witness is Stephen Lewis, Deputy Director for Personnel, Industrial and Physical Security Policy within the Office of the Under Secretary of Defense for Intelligence, United States Department of Defense. The Under Secretary of Defense for Intelligence oversees DOD's policies, programs, and guidance related to, among other things, personnel and facility security. Mr. Lewis also previously appeared before our Committee just about a month ago at our first hearing on the Washington Navy Yard hearing.

We welcome you all today, and before I ask Ms. Durkovich to lead off, I am going to yield to Dr. Coburn. Good morning.

## OPENING STATEMENT OF SENATOR COBURN

Senator COBURN. I apologize for being late, both to our witnesses and to the Chairman. I will put my opening statement in the record.[1]

Chairman CARPER. Fair enough. Welcome.

Ms. Durkovich, please proceed. Your entire statement will be made part of the record, and you are welcome to summarize as you see fit. Try to stick within about 5 minutes, but if you go a little beyond that, that is all right.

[1] The prepared statement of Senator Coburn appears in the Appendix on page 189.

**TESTIMONY OF CAITLIN A. DURKOVICH,[1] ASSISTANT SECRETARY FOR INFRASTRUCTURE PROTECTION, NATIONAL PROTECTION AND PROGRAMS DIRECTORATE, U.S. DEPARTMENT OF HOMELAND SECURITY**

Ms. DURKOVICH. Thank you very much, Chairman Carper, Ranking Member Coburn, Senator Heitkamp, and other distinguished Members of the Committee. I am pleased to appear before you today to help honor the memory of the 12 men and women who died at the Navy Yard and all of those who have been victims of violence in the Federal workplace.

As Assistant Secretary for Infrastructure Protection (IP), I have had the responsibility to lead the overall coordination of the Nation's critical infrastructure security and resilience efforts. One of the most rewarding opportunities I have is to serve as Chair of the Interagency Security Committee, and oversee the development of standards, reports, guidelines, and best practices for facility security at nearly 400,000 civilian Federal facilities.

The ISC was created by Executive Order (EO) following the bombing of the Alfred P. Murrah Federal Building in Oklahoma City on April 19, 1995. The ISC and its 53 member Federal departments and agencies is responsible for the creation and adoption of numerous standards, guidelines, and best practices for the protection of these nearly 400,000 non-military Federal facilities across the country.

The 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 facilities, the design and implementation of risk-based security policies.

Recently the ISC issued the Risk Management Process for Federal Facilities Standard, a standard that 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 facility security countermeasures for all non-military Federal facilities. The standard also provides guidance for customization of the countermeasures for Federal facilities and explains that risk may be addressed in various ways, depending on agency mission needs, for example, presence of a child-care center onsite and historical significance.

It is most important to note that the ISC is a truly collaborative interagency body. Fifty-three Federal departments and agencies participate in the ISC and take the lead on bringing ideas to the table in drafting standards and best practices. When agencies cannot solve security-related problems on their own, the ISC brings chief security officers and senior executives together to solve continuing governmentwide security concerns.

ISC membership also engages in the development of standards and best practices based on evolving real-world threats. Recent events have demonstrated the need to identify measures that can be taken to reduce the risk of mass casualty shootings and work-

[1] The prepared statement of Mr. Durkovich appears in the Appendix on page 192.

place violence, improve preparedness, and expand and strengthen ongoing efforts intended to prevent future incidents.

The Department of Homeland Security 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, countering improvised explosive devices (IEDs), incident response, and workplace violence. Working with partners in the private sector, DHS has developed training and other awareness materials to assist owners and operators of critical infrastructure to better train their staff and coordinate with local law enforcement for these types of incidents. We have hosted workshops and developed an online training tool targeted at preparing those who work in the buildings. These efforts and resources have been well received and are applicable to Federal facilities as well as commercial spaces and other government buildings.

Cognizant of this growing threat, the ISC this spring formed a Federal Active Shooter Working Group. While a number of Federal guidance documents previously existed on active-shooter preparedness and response, this working group was formed to streamline the existing ISC policy into a single cohesive document. To date, the working group has met five times and has reviewed numerous publications and guidance documents including training and materials developed by the Department for commercial facilities. It will also leverage lessons learned from real-world incidents, such as 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 and constantly evolving. Not only are there terrorist threats, like the bombing at the Boston Marathon this past spring or the complex shopping mall attack in Nairobi in September, but hazards from weather-related events such as Hurricane Sandy and a cyber infrastructure increasingly under attack all have a direct impact on the security of our Federal buildings. It is impossible to anticipate every threat, but 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 member departments and agencies ensures that those responsible for Federal facility security have the tools and resources to mitigate the threats.

In closing, I would like to thank you for the opportunity to appear before you and discuss the important work of the ISC and how we can learn from real-world events and ensure they do not happen again. I look forward to answering any questions you may have.

Chairman CARPER. Secretary Durkovich, thank you. Thanks for being here. Thanks for your testimony and your work.

General, welcome.

**TESTIMONY OF LEONARD ERIC PATTERSON,[1] DIRECTOR, FEDERAL PROTECTIVE SERVICE, NATIONAL PROTECTION AND PROGRAMS DIRECTORATE, U.S. DEPARTMENT OF HOMELAND SECURITY**

General PATTERSON. Good morning. Thank you, Chairman Carper, Ranking Member Coburn, and Senator Heitkamp. 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.

FPS is charged with protecting and delivering integrated law enforcement and security services to over 9,000 facilities owned or leased by the General Services Administration and safeguard their more than 1.4 million daily occupants and visitors.

In performing this mission, FPS directly employs over 1,000 law enforcement officers , inspectors, and special agents who perform a variety of critical functions, including FPS-contracted protective security officer oversight, facility security assessments, and uniformed police response.

Our inspectors and special agents receive extensive and rigorous training at the Federal Law Enforcement Training Center (FLETC) and in the field. This training ensures that our law enforcement personnel are able to effectively respond to tens of thousands of calls for service received annually by the FPS and conduct thorough, comprehensive facility security assessments in FPS-protected facilities.

The Facility Security Assessments (FSAs), document security-related risk to a given facility and provide a record of countermeasure recommendations designed to enable tenant agencies to meet Interagency Security Committee standards for Federal facility security. Throughout the FSA process, FPS works with stakeholders to identify and gather all necessary information for characterizing the risks unique to each facility. FPS then builds a consensus with tenant agencies regarding the type of physical countermeasures and number and type of guard posts staffed by FPS-contracted Protective Security Officers (PSOs) appropriate for each individual facility.

Approximately 13,000 FPS-contracted PSOs staff guard posts at FPS-protected Federal facilities. 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. In fact, FPS PSOs stop approximately 700,000 prohibited items from entering Federal facilities every year.

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 crime scene protection, actions to take in special situations such as building evacuations, safety, and fire prevention, and public relations.

[1] The prepared statement of Mr. Patterson appears in the Appendix on page 198.

All PSOs must undergo background investigation checks to determine their fitness to begin work on behalf of the government and are rigorously trained. However, it is important to note that PSOs are not sworn law enforcement officers. Rather, PSOs are employees of private security companies, and FPS does not have the authority to deputize PSOs in a law enforcement capacity. An individual PSO's authority to perform protective services are based on State-specific laws where the PSO is employed.

To ensure high performance of our 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 personnel files are audited periodically to validate that PSO certifications and training records reflect compliance with contract requirements. In fiscal year (FY) 2013 alone, FPS conducted 54,830 PSO post inspections and over 17,000 PSO personnel file audits.

The Federal Protective Service is committed to providing safety, security, and a sense of well-being to thousands of Federal employees who work and conduct business in our facilities each day.

We continuously strive to further enhance, integrate, and transform our organization to meet the challenges of an evolving threat landscape and have recently made significant progress toward closing out outstanding the Government Accountability Office (GAO) recommendations pertaining to FPS operations. In fiscal year 2013 alone, FPS submitted documentation to the GAO for closure and consideration pertaining to 13 GAO recommendations including FPS strategies to enhance its human capital planning and improve tenant communication. Of those presented, six were successfully closed as implemented, and seven are pending GAO's internal review for closure.

Significant progress has also recently been made toward closing longstanding GAO recommendations related to FPS' handling of PSO training and oversight. While challenges undoubtedly remain, FPS has successfully closed six outstanding recommendations directly related to this program area and is pending GAO's internal review process for closure consideration for two more.

We have also made advances toward addressing recommendations relative to our risk-assessment methodology. Specifically, FPS designed its FSA process to meet the requirements of the ISC's Risk Management Process for Federal Facilities and, to ensure that stakeholders have an understanding of the threats they face, FPS has begun to provide a Threat Assessment Report as part of each FSA. Going forward, FPS will continue to work with the ISC to explore consequences and impacts in the context of Federal facility security assessments and explore the inclusion of consequences into the FSA process.

In closing, I would like to acknowledge and thank the distinguished Members of this Committee for the opportunity to testify today, and I would be pleased to answer any questions you may have.

Chairman CARPER. Thank you, General.

Mr. Lewis, welcome. Good to see you. Please proceed.

**TESTIMONY OF STEPHEN F. LEWIS,[1] DEPUTY DIRECTOR FOR PERSONNEL, INDUSTRIAL AND PHYSICAL SECURITY POLICY, DIRECTORATE OF SECURITY POLICY AND OVERSIGHT, OFFICE OF UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE, U.S. DEPARTMENT OF DEFENSE**

Mr. LEWIS. Good morning. Thank you, Chairman Carper, Ranking Member Coburn, and Senator Heitkamp. I appreciate the opportunity to be here today to address the practices and procedures in the Department of Defense regarding facility security. I am Steve Lewis, Deputy Director of the Security Policy and Oversight Directorate in the Office of the Under Secretary of Defense for Intelligence, and I am here today on behalf of Dr. Michael Vickers, the Under Secretary of Defense for Intelligence, or (USD(I)).

The USD(I) is the Principal Staff Assistant to the Secretary and Deputy Secretary of Defense for security matters and is responsible for setting overall DOD physical security policy. In this role, the USD(I) provides security policy standards for the protection of DOD personnel, installations, facilities, operations, and related assets.

Within the Department, the USD(I)'s security responsibilities are complemented by those of the Assistant Secretary of Defense for Homeland Security and Americas' Security Affairs, who is responsible for the DOD Antiterrorism Program.

In the wake of the tragic Washington Navy Yard shooting incident, the Secretary of Defense initiated concurrent internal and independent reviews to identify and recommend actions that address gaps or deficiencies in DOD programs, policies, and procedures regarding security at DOD installations. The reviews also cover the granting and renewing of security clearances for DOD employees, military service members, and contractor personnel.

In order to address the Department's facility security policies and practices, it is first important to describe the requirement for military commanders, or their civilian equivalents, to conduct a comprehensive security evaluation of a facility or activity. The purpose of this evaluation is to determine the ability of the installation to deter, withstand, and recover from the full range of adversarial capabilities based upon a threat assessment, compliance with established protection standards, and risk management. Based upon the results of these evaluations, active and passive measures are tailored to safeguard and prevent unauthorized access to personnel, equipment, installations, and information by employing a layered security concept known as "security-in-depth."

The Department requires the development and maintenance of comprehensive plans to address a broad spectrum of natural and manmade scenarios. These include the development of joint response plans to adverse or terrorist incidents, such as active shooters and unauthorized access to facilities. Military commanders, or their civilian equivalents, using risk management principles, are required to conduct an annual local vulnerability assessment and are subject every 3 years to a Higher-Headquarters Assessments, such as the Joint Staff Integrated Vulnerability Assessment (JSIVA).

[1] The prepared statement of Mr. Lewis appears in the Appendix on page 205.

The Department has worked very hard to foster improvements that produce greater efficiencies and effectiveness in facility security. In its continuing efforts to harmonize its facility security posture with other Federal departments and agencies, military commanders located in DOD-occupied leased facility space—primarily those not on a DOD installation, must utilize the Federal Interagency Security Committee's Risk Management Process for Federal Buildings. This effort includes the incorporation of the ISC's physical security standards in DOD guidance, for example, the Unified Facilities Criteria.

DOD also participates in various interagency fora such as the Interagency Security Committee, along with representatives from the Department of Homeland Security and many other Federal agencies and departments. These fora enable the sharing of best practices, physical security standards, and cyber and terrorist threat information in support of our collective resolve to enhance the quality and effectiveness of physical security of Federal facilities.

We also have various ongoing initiatives across the Department to enhance facility security, such as the development of an Identity Management Enterprise Services Architecture (IMESA). IMESA will provide an enterprise approach to the sharing of identity and physical access control information and complement ongoing continuous evaluation concept demonstration efforts. IMESA will provide real-time vetting of individuals requiring unescorted access to DOD facilities, and these will be run against DOD, Federal, State, and other authoritative data sources. IMESA users will be able to authenticate individuals' access credentials and fitness to enter the facility. We believe that IMESA will vastly enhance the security of DOD personnel and facilities worldwide.

Thank you for your time. I am happy to take your questions.

Chairman CARPER. Thank you, Mr. Lewis. I am going to call on Dr. Coburn for the first questions, and then I will yield to Senator Heitkamp and then follow her. Dr. Coburn.

Senator COBURN. General Patterson, go through again the GAO recommendations that you all have now met and when they were met, because my understanding was that of the 26 GAO recommendations between 2010 and 2012, prior to the Navy Yard shooting, only four of those had been acted on. Is that correct?

General PATTERSON. No, sir. I can get you a listing of all of the specific recommendations.

Senator COBURN. In your testimony, you listed several. Would you do that again for me?

General PATTERSON. I do not think I listed them specifically, sir.

Senator COBURN. You said numbers, and that is the numbers I want.

General PATTERSON. Yes, sir, and I can get you the specifics behind the different recommendations. I do not have the recommendations before me right now. But the numbers are accurate.

Senator COBURN. But there were 26 outstanding GAO recommendations between 2010 and 2012.

General PATTERSON. I would have to find that, sir.

Senator COBURN. And four of them had been acted on and accomplished based on their recommendations, and you gave a litany of others that you have acted on.

General PATTERSON. Yes, sir. I was giving you a general oversight of the number that we had been——

Senator COBURN. Yes, well, go back to your testimony and give that to me again, would you?

General PATTERSON. Yes, sir, I sure will.

In 2013, FPS submitted documentation to the GAO for closure and consideration pertaining to 13 GAO recommendations including FPS strategies to enhance its human capital planning and improve tenant communication. Of those presented, six were accepted and closed as implemented, and seven are pending GAO's internal review for closure.

Senator COBURN. So that is half of them, of the 26.

General PATTERSON. Yes, sir.

Senator COBURN. So my question to Secretary Durkovich: Were you aware at the National Protection and Programs Directorate that there were 26 outstanding recommendations made by GAO and that up until the first of 13, only 4 had been acted on?

Ms. DURKOVICH. Thank you for the question. Yes, I am aware of the various GAO recommendations that are open and that have been closed. Just from a more high level standpoint, the Department has initiated an overall effort to make sure that all of the open GAO recommendations that the various components and subcomponents work closely with GAO to address those recommendations and to take steps to close them. So——

Senator COBURN. When did you all initiate that?

Ms. DURKOVICH. So as recommendations are provided to us by GAO, we begin our work to——

Senator COBURN. I understand that, but you just said you initiated a process where they would be addressed.

Ms. DURKOVICH. That is a standard process within the Department. Again, when we receive a recommendation from the GAO, first of all, we have to submit a letter about whether we agree or disagree with the recommendation——

Senator COBURN. Right. I understand that.

Ms. DURKOVICH [continuing]. And that begins the process. I do not have specific oversight over the FPS recommendations. As the Assistant Secretary for the Office of Infrastructure Protection, I handle the recommendations that are specific, for example, to my programs, including the ISC. So we have five open GAO recommendations, and we work very closely to document what we are doing to address those recommendations and provide regular updates to the GAO through letters to, again, document what we are doing and the timeline for which we think that we will meet the mitigation measures or the measures that we have taken to address the recommendations.

Senator COBURN. See if I have this right, because I may not. The Interagency Security Committee does not monitor agencies for compliance. Is that correct?

Ms. DURKOVICH. Based on the Executive Order, departments and agencies shall comply with the standards that are produced by the Interagency——

Senator COBURN. I understand that.

Ms. DURKOVICH [continuing]. Security Committee.

Senator COBURN. But what I am asking is they do not monitor the individual agencies to see if they are in compliance. There is an Executive Order——

Ms. DURKOVICH. We do not specifically——

Senator COBURN [continuing]. That says the agencies are supposed to do it, but ISC does not monitor to see that that happens. Is that correct?

Ms. DURKOVICH. That is correct, yes.

Senator COBURN. And it is the responsibility of each individual agency to make sure they comply with that.

Ms. DURKOVICH. Yes. Based on the Executive Order, yes, sir.

Senator COBURN. So let us go back to FPS for a second. How is it that your agency is complying with the standard set by the ISC?

General PATTERSON. Well, sir, we do work with our Federal partners as we go in and do assessments. We will make recommendations as they are outlined by the ISC, and for a variety of reasons, a Federal partner may or may not be able to implement. It could be because of cost. It could be because of a variety of things that they may decide that they cannot meet those specific recommendations.

However, once we do understand that they are not able to, we have tried to work with them to try to mitigate those shortfalls as much as we can. So it is not as if we walk away from that.

Senator COBURN. No. I am not saying that. I am just—for example, active-shooter training, all right?

General PATTERSON. Yes, sir.

Senator COBURN. A large proportion of our officers that we either contract or have are not trained.

General PATTERSON. Yes, sir, and if I may explain, there is a reason for that, and the reason is because historically, as I stated in my testimony, active-shooter response, not awareness but active-shooter response, has been a function of law enforcement, period. Our PSOs are not law enforcement officials. And so to put them in a position to where they are responding as a law enforcement officer requires at least our coordination with the State, and there has to be some contractual agreement that they will respond in that manner.

Now, because we recognize that in some instances our PSOs will be the only folks in a particular position to respond in a prompt manner, we are now working with the National Association of Security Companies (NASCO), to look at how we can provide training to where they can apply some response. But the bottom line is we still want law enforcement folks to respond because that is where they are trained. We spend any number of hours with our inspectors and our agents in learning how to respond to an active-shooter situation, and we have not done that with our PSOs. So we have to find out what the happy medium is here so we do not put our PSOs in harm's way as well. So we need to find out what the right level of training would be for them in order for them to respond effectively.

Senator COBURN. So we have security personnel at Federal buildings, but if we have an active shooter, we do not want them to re-

spond; right now they are not trained in a way to handle that situation.

General PATTERSON. Here is what they are trained in, sir: They are trained to protect the people and to keep people from coming in the building so that they do not enter harm's way. They are also trained to help people evacuate in a very timely manner. And if, in fact, they are approached or come in contact with a shooter, they are trained to engage.

What they are not trained in is to go find the shooter and then take action.

Senator COBURN. So they are trained to engage?

General PATTERSON. They are trained to engage. Yes, sir.

Senator COBURN. And all of them are?

General PATTERSON. Yes, sir.

Senator COBURN. OK. I am past my time. Thank you.

Chairman CARPER. Thank you. Senator Heitkamp.

Senator HEITKAMP. Thank you, Mr. Chairman.

The first obligation of any employer is safety. I think you will find that in a lot of facilities across the country, whether they are a manufacturing plant or a processing plant of any type or even in a major office. It is not only good employee management, it actually saves a lot of money. And I think this Committee is deeply concerned about the safety of public employees in buildings, and certainly the Navy Yard is yet again another example where we do not live in a perfect world, but were there things that could have been done, that should have been done differently that would have either prevented it or limited the deaths once the shooting began?

I want to go back to a couple kind of critical points here, which is even though we have Executive Orders and we have all of the GAO reports and all the recommendations, it is kind of like the words get written but no one is responsible for followup, no one is responsible for implementation, no one is responsible to the public employees to say yes, we have done everything that we can, we know what the path forward is that will enhance your safety. But we just made these recommendations, and we hope that whoever manages that building or whoever runs this agency is taking safety as seriously as what we do.

And so I will tell you I am concerned listening to this that there does not seem to be a lot of coordination, and even when there is coordination, there is not a lot of followup in terms of making sure that these things get done.

I want to go back to maybe what I am not understanding is the engagement of an active shooter. I chaired a task force when I was Attorney General (AG) on school safety. We made everyone in the building have training. Our recommendation, which was carried out by many schools across this country, is that we train on what happens if there is an active shooter. And the person we found out we needed to train, give the clearest training to, was the woman who answered the phone or the man who answered the phone at the reception desk. And obviously in most Federal buildings the first person you are going to encounter will be someone in uniform, General, that is under your jurisdiction. And so what recommendations would you make to change what you are currently doing in an active-shooter situation?

General PATTERSON. Yes, ma'am. As an agency we have thought long and hard about this. We have been working very diligently with our vendors to take a look at where we need to be in helping them and helping us to understand: how do we go forward and proceed forward now in the training? What training do we need to provide, what level of training do we need to provide for our PSOs?

Senator HEITKAMP. Have you considered that maybe someone who is law enforcement trained and authorized to engage at a much higher level should be on duty, not always to do the scanning and the screening and, the kind of day-to-day but have someone there who actually has a role in providing protection?

General PATTERSON. Yes, ma'am, we would love to. I have about 600 inspectors who are law enforcement officials who are in a number of our buildings on a regular basis. But we have thousands of buildings, so I cannot put law enforcement folks in every building.

We have great relationships, with State and local authorities that we can call on very quickly to respond if we have a problem. But at this point, ma'am, I do not have the resources that would allow us to put a law enforcement individual in these facilities.

Now, there is a possibility that we could possibly deputize some of our contractor personnel. However, that would clearly be more costly, and we would have to figure out how we would do that.

Senator HEITKAMP. It is troubling that there does not seem to be a lot of kind of creative thinking on how we can use the resources we have more effectively to protect folks. And, Mr. Lewis, obviously this is a great tragedy, and I know very many people within your sphere are still dealing with the extent of this tragedy. But I would suggest that maybe the best way we can deal with this tragedy is assure people we have learned the lessons. And so can you tell me what lessons your agency has learned from this? I know you are undergoing this review, but give us a little peek into what the thinking is right now.

Mr. LEWIS. Well, since we talked a little bit about active-shooter awareness and training, within the Department we have incorporated active-shooter awareness into the antiterrorism level one training. So that has been introduced throughout the DOD population.

In addition, we have published Workplace Violence and Active Shooter Prevention and Response, and this was in response to the Fort Hood incidents. So we have measures in place to not only deal at an awareness level but in terms of response within the Department.

Since the Washington Navy Yard tragedy, we have really focused on continuous evaluation of our cleared and vetted personnel, so not just people who have security clearances but also people who are eligible to have access to DOD installations. And you can do the best investigation possible, but things change in people's lives over time. And we have to be constantly aware of what those changes are, and we have established a pilot on continuous evaluation, which is going to do queries, automated queries of public and DOD records to look for issues of concern. And this is an ongoing effort. We are trying to expand it to include individuals who are visiting installations on a fairly regular basis. That was the IMESA initiative that I mentioned, which would, in an automated fashion,

allow for sharing of information of concern between DOD facilities so that if a visitor to one DOD installation presented a problem there for whatever reason, that would be available to other DOD installations that that person may be going to visit.

So that is our focus. How do we become apprised of information as it develops and not wait 5 years or 10 years for the next reinvestigation?

Senator HEITKAMP. If I can just make a comment, I think honestly I would like to see better coordination, and I would like to see better followup when GAO has a number of recommendations that sit around for a number of years, and we come and we say, "Well, yes, we are working on it." That just is a constant source of frustration on this Committee. "We are working on it," or, "Yes, we are concerned about it," does not cut it anymore, especially when we are talking about safety of public employees and really the integrity of your missions. And so I would like to see maybe followup on the GAO recommendations, what the timeline is for actually getting those implemented.

Ms. DURKOVICH. May I take a moment just to address the coordination issue?

Chairman CARPER. Sure. Go ahead.

Ms. DURKOVICH. And I just want to go back to the Interagency Security Committee and reiterate that for over the last 17 years we have had the chief security officers and other senior executives from 53 different departments and agencies who participate as part of the committee and look at evolving threats and evolving hazards and work together to produce standards and best practices, whether it is on occupant emergency plans, whether it is on prohibited Federal items in Federal buildings, whether it is on the training of Federal Security Committees, and certainly the risk management process that we released this past August. It is a highly collaborative body, and while there is not a formal compliance mechanism, the fact that these 53 chief security officers come together and work over months to produce these standards, it then becomes incumbent on them to ensure that their facilities adopt them.

We have some informal soft compliance mechanisms that we are looking at. There are tools that are in development to help us better assess how facilities are implementing our standards and best practices, but I want to dispel the myth that it is not highly collaborative.

Certainly coming out of the Navy Yard and other incidents in Federal facilities, we have established an Active Shooter Working Group, as I mentioned in my opening statement, both designed to look at what happened at the Navy Yard but to leverage all of the work that we have done over the course of the last 6 years in the commercial facility space. We have online training, we do in-person training, and part of the goal here is to look at all of the various tools, documents, trainings that are available right now, to leverage those so we can bring them to the Federal workplace. I think training is a very important aspect of this. It is certainly something that Director Patterson does as part of his responsibilities. But there are other things, I think, that we can do to augment that, to answer your question, and to ensure that as we look at developing, whether it become a best practice or a standard, that we are en-

couraging and recommending that we exercise, that we test the training that we do, that we ensure that there are documents, that there are marketing materials available to our employees. But I think that there is a lot that can be done and that can be leveraged from the work that we have already done with the commercial facilities sector, and that is certainly the goal of our Active Shooter Working Group.

Chairman CARPER. Senator Heitkamp, we are blessed on this Committee to have several Members of the Committee who have served as Attorney General in their own States, and thank you for bringing that expertise to bear here.

Secretary Durkovich, I am going to ask you to help make real for me and maybe for some of my colleagues this Interagency Security Committee. Just cut through the—not that you are using jargon. Just cut through the Federal verbiage and just say where did it come from, why did we create it. Just describe its mission or missions. And maybe more importantly, how do you think it is working? How do we measure whether it is working well? How do we measure success? Please, just make it real for us.

Ms. DURKOVICH. Absolutely, and thank you for the opportunity to further explain it. So the Interagency Security Committee came about after the bombing at the Alfred P. Murrah Building in Oklahoma City in 1995, with the recognition really that we had to do a better job protecting our Federal facilities. Again, almost every department and agency participates in the Interagency Security Committee, and it is often the most senior physical security person within that department, the chief security officer.

We take evolving threats and evolving challenges, and it is the chief security officers who look at the particular threat and decide how do we, as a Federal family, best address that threat and make sure that our facilities are able to mitigate them. So there is a formal risk management process that the committee has produced, and it is the standard by which we go about securing all Federal civilian facilities with the exception of DOD military installations. And it begins with determining what is the facility security level. So you look at a particular Federal facility, and based on what its function is—is it a headquarters office? Is it a field office? Does it have historical significance? For example, is the Declaration of Independence or the Bill of Rights contained in it? Are there other ancillary functions? Are there child-care facilities and things? That is what allows us to determine whether a facility is either a Level 5, which is the highest level, or a Level 1, which is more of your storefront office.

Then we apply the physical security criteria. So based on the level and also what we call the design-basis threat standard, that is 31 undesirable events that we have determined are most attractive or most likely to happen to a Federal facility, and it ranges from arson to sabotage to active shooters and also weather-related events. But based on those scenarios, what are the right security measures to put in place at these Federal facilities?

Now, it is a risk-based process, and as you pointed out in your opening statement, it is difficult at times to apply all of these because, as you have noted, not all buildings were built 100 or 150 years ago with a 15-to an 18-foot setback. We have to think about

how you mitigate some of these vulnerabilities based on the real-world realities. And so we help provide facilities with options to include bollards, thinking about blast-resistant windows, but really working them through this risk management process. The establishment of facility security committees, and ensuring that the individuals that sit on those committees have the training that they need to carry out their duties is a core part of, again, what the Interagency Security Committee has thought about and how we—again, when there are unique functions inside a building, how do we ensure that we are also protecting those functions? And, again, that is things like child care and other high-priority efforts.

So that is really the basis for what the Interagency Security Committee does, and again, thinking about how we keep those standards fresh, how we recognize that we are living in a world where our adversaries are highly adaptive. So when we start to see emerging threats or new trends, again, we bring the 53 chief security officers together to come up with a standard to ensure that all Federal facilities at least are working from a certain baseline, and we are doing that with active shooter. We are thinking about as we start to see some of these small-scale complex attacks, how are we accounting for them? And, again, how do we ensure that we have the measures, the training? We have done the preparedness so that we can mitigate the threats.

I do think——

Chairman CARPER. Let me just interrupt. Come back—and you may have said this and I missed it, but, again, how do you measure success? What metric are we using to measure whether or not the work of the Interagency Security Committee is successful?

Second, talk with us about sharing, the sharing of best practices across the range of the Members who comprise this committee. Two things.

Ms. DURKOVICH. Absolutely. So I will answer your first question by saying I do think that the Interagency Security Committee has been a success, and I think that if you—and we have done informal surveys, but if you went out and surveyed each of the Federal departments and agencies, you will find that they have implemented all of the ISC standards. If there is——

Chairman CARPER. And you said those standards continue to be updated. Is that right?

Ms. DURKOVICH. And they continue to be updated. And, again, they are the ones who come together to help develop these standards. We do not have a formal mechanism for measuring what has been implemented. There is one ISC-approved tool that is in existence. We are working on approving others. But anecdotally I would—again, I am confident that all of the member departments and agencies have implemented the standards, and when they cannot, they are responsible for coming to us and telling us why they cannot and the fact that they are willing to bear that risk.

Chairman CARPER. Talk with us about sharing best practices across departments.

Ms. DURKOVICH. Absolutely. Again——

Chairman CARPER. And how, if at all, this committee facilitates that.

Ms. DURKOVICH. One of the benefits of the Interagency Security Committee is that you may have a chief security officer who represents a Level 5 facility who can come and talk about some of the things that they have done. Take, for example, a headquarters building that sits on Constitution Avenue. The things that they have put in place to mitigate the fact that they cannot have a setback, the fact that they use bollards, the fact that they use, again, blast-resistant windows. So part of, again, the very nature of the Interagency Security Committee is the fact that we can bring together and we can convene these senior-level executives to talk about best practices. But I think what is unique about what we are doing with the ISC is it is not just the sharing of Federal facility best practices, but the fact that for over the course of the last 6 years, we have been working very closely with the commercial facilities sector. These are buildings, these are stadiums, these are venues where the public passes through them day in and day out, where we have done active-shooter training, where we have thought about how do you, again, strengthen and provide layers of security that may not always be obvious to the public. How do we take those lessons learned, how do we take those best practices and bring them to Federal facilities as well?

And so I think as part of the Active Shooter Working Group that we have stood up, you are going to see a mix of both what we are doing in the Federal sector but also the lessons learned, the leading practices that we have developed in the commercial facilities sector as well.

Chairman CARPER. OK. Thanks. Dr. Coburn.

Senator COBURN. Just to followup, I want to put in the record a letter from the DHS Police Deputy Director of Operations Kris Cline[1] that was released November 22, which is new Active Shooter Guidelines.

And I am somewhat confused after reading this, and I do not understand the engagement. If somebody is with a firearm in a Federal building and we have a PSO officer there, nothing here says that they will engage them.

General PATTERSON. Yes, sir. The original objective and mission of the PSO was to ensure the safe egress and ingress of people coming into the facility. It was not to pursue an active shooter. That has always been the purview of and the ground for trained law enforcement personnel.

As we have looked at how we might have our PSOs engage, we were looking at any legal obstacles that we may have to overcome as a result of that, as well as any State requirements that they may have to meet as well. So my point in talking about it is if an armed individual comes into that facility and they recognize that they are armed and they ask that individual to please drop their gun or drop their weapon or put the weapon down and they do not, then they are authorized to engage.

If, in fact, they are clearing the building or trying to get people out of the building and then they run into that active shooter, they will engage.

[1] The letter from Kris Cline appears in the Appendix on page 254.

What they are not trained to do is go from room to room trying to find the individual.

Senator COBURN. I understand that, but I guess my point I am making from this letter, that is not clear in here. This is the new requirements for active shooters.

General PATTERSON. Yes, sir.

Senator COBURN. That is not a clear part of this statement.

General PATTERSON. Yes, sir. And since that was dated in November, and in early December, we had a conversation with most of our vendors, telephonically, to tell them that we would be coming out with new instructions about how they would engage and to be prepared for that. So, yes, sir, it is evolving.

Senator COBURN. OK. So right now, if an event happened today, they would be following this, not what you testified?

General PATTERSON. No, sir. They would continue to engage. Their first priority is the safety of the folks that are in that building. So they are going to keep people from coming in, and they are going to help folks to get out.

Now, if they come into contact with a shooter, they will engage. What they will not do today is pursue the active shooter.

Senator COBURN. I understand that.

General PATTERSON. Yes, sir.

Senator COBURN. What I am saying is it is not clear to me in terms of reading this letter that says they will engage.

General PATTERSON. OK. I will have to take a look at that.

Senator COBURN. Well, this is what you all put out November 22, and that is the important thing.

One other area I want to cover with you, General Patterson. Do we direct FPS-contracted security to do joint exercises with local law enforcement? In other words, a dry run—much like Senator Heitkamp said.

General PATTERSON. Yes, sir. What we do is when we conduct an exercise, we conduct a lot of exercises—in fact, we conduct a number of active-shooter training exercises in Federal——

Senator COBURN. You are missing my point. Do we require our contractors——

General PATTERSON. Yes, sir. I was going to get to that.

Senator COBURN [continuing]. To do joint training with local law enforcement?

General PATTERSON. Well, they will do it when we do it.

Senator COBURN. No. But I am saying, is it a requirement of their contract to do joint training with local law enforcement so that we have dry runs, so that everybody is coordinated, going back to what Senator Heitkamp said?

General PATTERSON. Right. Yes, sir. Their exercise will be part of our exercise as we practice with local law enforcement.

Senator COBURN. OK. But you are not in every one of these buildings, and you are not going to have an exercise in every one of these buildings.

General PATTERSON. That is true.

Senator COBURN. As a matter of fact, that is what the record shows.

General PATTERSON. That is true.

Senator COBURN. So is it not the fact that you have actually directed these contractors not to do joint training with local law enforcement?

General PATTERSON. No, I would not say that we have directed them not to do joint training. The fact is, Senator, at this point we do not have anything specifically that addresses joint training with local law enforcement in our contracts. But I will have to get back with you on that. I do not have the contract before me, so I would have to take a look.

Senator COBURN. Senator Heitkamp.

Senator HEITKAMP. I was not intending on following up, but I do want to kind of pick up from where Senator Coburn has taken the discussion, which is security is—I guess if I can just say it this way—best done when it is clear that this is a high priority. And, it concerns me that public employees and really the public see someone sitting at a desk, and they are usually uniformed, and there is an assumption that there is a bevy of powers that comes with that and that there is an aura of protection that goes with that. And if it does not include engagement, if it does not include having folks who are at least capable of some kind of immediate intervention, and if those roles are not clear, I think we have left the wrong message with a lot of people in the public.

And so I would like to know—for many of these buildings, there was not any kind of electronic screening or X-ray machines at the Navy Yard. Correct?

General PATTERSON. I do not know.

Senator HEITKAMP. You could just walk—I mean, if you scanned in through the turnstile and, kind of waved and signed in and that was it, right?

Mr. LEWIS. Yes.

Senator HEITKAMP. OK. Now, this is a building that has thousands of public employees. I can understand that if you are looking at the building that houses the public employees for the Farm Service Agency in Watford City, North Dakota, you might not want to put any kind of screening device. But for a building that houses and employs—where thousands of employees come, it seems like there might be some cost/benefit in safety in looking at electronic surveillance. There might be some cost/benefit in providing law enforcement-trained people at the front to engage, that we might look at those kinds of procedures. And I do not hear that today.

I thought I was going to hear that we are looking, doing cost/benefit analysis, and it is not that my folks in Watford City are not important. But I do not expect you to hire a law enforcement-trained guard to protect the one person that works there. I do not expect that. But I might expect you to think about doing that in a building that houses thousands of people in a city that frequently is a target symbolically of terrorism or these kinds of attacks.

I really would ask you guys to just go back and rethink what you are saying today about how you can enhance security looking beyond simply kind of continuing the process that you have engaged in today.

General PATTERSON. Ma'am, if I could address your concerns just for a minute. We are actually doing due diligence in pursuing this matter. We are working aggressively with the vendors, one, to look

at what authorities the States entitle them to relative to engagement. We are also looking within the Department to look at what authorities might be levied where we could render to these folks relative to legally from the Federal sector. So we, in fact, are looking at how we might address this moving into the future, because we realize it is a concern.

One of the other things that I spend a lot of time doing is engaging with the Federal executive boards across the country, looking at what are some of the challenges that they are having, what are the concerns from their people in these facilities, and how can we provide better training, more training, additional training to those folks in the facility as to how to respond to an active shooter, because that is very important as well. How do we get people out of harm's way when they recognize that there is an event in progress?

So I would tell you we are looking at this. We are taking it very seriously. It may not come across that way in some of the testimony that we are providing, but I can tell you that we are spending a lot of time with our contractors, a lot of time with legal, to find out what is that middle ground, what is that ground that we can take, because ultimately we have to figure out who is going to bear the cost of this. And how can we do this in fundamentally a smart way, an effective way, an efficient way, but still provide the same result or similar result of protecting the folks in those facilities?

Senator HEITKAMP. All right. Not to belabor this, but it just seems like if I were looking at this and I was sitting in any of your shoes, I would say I have 1,000 people that work in a building in a city that is a target. We do not have screening devices, and we do not have law enforcement-trained guards. Maybe we ought to rethink that as a strategy.

Ms. DURKOVICH. So if I may address that, when we set the facility security level, as part of the recommended security practices, if you are a Level 3 or above, for example, we will at a minimum recommend that there are guards onsite at the facility. As you move up, so, for example, in any of the headquarters buildings again that you see along Constitution Avenue, you will find advanced screening techniques—magnetometers, you have to run your bags through—similar to what happened when we walked in the building today.

To your point, as we go down to those storefronts out in the States, that is where you will not see that level of security. But based on what your facility security level is, there is a standard that goes with that security, and that is part of what the Interagency Security Committee does, is make recommendations. And, again——

Senator HEITKAMP. Secretary, back to that point, you make recommendations, and there is no mechanism to mandate that those recommendations are carried out. Is that what we are hearing today?

Ms. DURKOVICH. We do not have a formal compliance mechanism to monitor what has been adopted, yes.

Senator COBURN. If I may, I just want to clarify. General, what I am asking you specifically on the GAO recommendations is the

dates at which you submitted, the dates that were cleared on just the 2010 through 2012 GAO recommendations.

General PATTERSON. 2010 to 2012.

Senator COBURN. And then a question for Secretary Durkovich. Is it public knowledge what Federal buildings are rated what? Can I go on a website somewhere and find that out?

Ms. DURKOVICH. It is not public knowledge.

Senator COBURN. So I could not find——

Ms. DURKOVICH. We can make that available to you, but it is not public, no, because it presents a security risk as well.

Senator COBURN. Sure. I understand that. That is why I asked the question. Thank you.

Chairman CARPER. I want to stick with the matter of GAO recommendations. GAO does very good work. They have a lot of people, but they have a whole lot of work to do, and they frankly have not been getting the kind of resources they need to do all that we are asking them to do.

Just describe for me, one or both of you—we will start maybe with General Patterson. Explain to us the process. GAO comes in. They are looking at the work that is being done, how it is being managed, funded, and so forth. And they make recommendations. Just describe the process, the give-and-take before they actually finalize their recommendations, please.

General PATTERSON. I am sorry. Could you——

Chairman CARPER. The process, just describe for us the process whereby GAO comes in, examines what is being done.

General PATTERSON. Right.

Chairman CARPER. Makes tentative recommendations. You have the opportunity, I presume, to respond to that, and then they finalize that.

General PATTERSON. Yes, sir.

Chairman CARPER. What we do here, we use the GAO recommendations, especially their high-risk lists that they put out at the beginning of every 2 years. We almost use it as a to-do list for us as we do our oversight and work in conjunction with them. Just describe the back-and-forth that leads to the issuance of a recommendation. I think you said there were 26 of them that you mentioned?

General PATTERSON. Yes, sir.

Chairman CARPER. And about 13 of them have been responded to.

General PATTERSON. Yes.

Chairman CARPER. And about half of those 13 have been, if you will, accepted. I am just interested in the process.

General PATTERSON. Yes, sir. Well, the process, when the GAO makes a recommendation, one of the first things that we do is we sit down with my staff to take a look at what is the genesis and what is the challenge here and what is the background on the recommendation. And then we move forward to look at how we are going to resolve the challenge that GAO has brought forward.

What I have recognized is that some things we can handle and move forward pretty quickly. Other things not so, only because it would require extensive resources and we have to figure out how we do that.

For instance, one of the challenges that we have is that we have 13,000 PSOs, guards, that we have oversight responsibility for, but we do not have the technology right now available to oversee them when they come to work, when they check in, and when they leave, to make sure that their certifications are up to where they need to be and so forth.

So one of the challenges that I have set forth for my staff and for the agency is to come up with a technology-based system that will allow us to move forward with that, to figure out when a PSO is on post, when he swiped in, when he swiped out, and to ensure that he or she has the proper certifications because that is one of the challenges that GAO has brought forward, because we only have 600 law enforcement folks out there to do this for 13,000 guards, it presents a bit of a challenge.

These 13,000 guards probably generate about 170,000 records that we must review over a period of time. So what we are looking for is an automated process to help with that. So we are engaged with DHS Science and Technology to help us begin to look for ways, and some off-the-shelf technology possibly, recommendations that we can begin to put into place that will allow us to better oversee these 13,000 guards.

So it is challenges like that that keep us from moving forward as expeditiously as we would like to.

Senator COBURN. Let me raise a question about that. You have 13,000 contracted guards.

General PATTERSON. Yes, sir.

Senator COBURN. And you have 600 people working directly for you——

General PATTERSON. Yes, sir.

Senator COBURN [continuing]. That are law enforcement officers.

General PATTERSON. Yes, sir.

Senator COBURN. That is less than 22 people a person.

General PATTERSON. Yes, sir.

Senator COBURN. We need an automated system to do that? What about random audits? How about firing a contractor who does not perform?

General PATTERSON. We do random audits, sir. Every one of my regions is responsible for doing 10 percent to 20 percent random audits per month. Part of the challenge, though, sir, is that because there are so many records, we can do an audit today, but tomorrow or within the next month, the individual may lose his certification based upon expiration of time or having to recertify and so forth. So allowing us to automate our records would help us tremendously in better overseeing this process.

Senator COBURN. Why should you automate it? Why shouldn't you force your contractors to automate it and present it to you?

General PATTERSON. That is an option, yes, sir.

Senator COBURN. It is not an option. It is the only common-sense thing you would do. If you want to contract with the Federal Government, you will demonstrate that the people that you have there are certified and compliant. And then you audit whether or not they are telling you the truth rather than spend a whole bunch of money, us running all 13,000 people when they are really not our

employees. They are contract employees for somebody that took a contract to guard a building. Again, it goes back to contracting.

General PATTERSON. Yes, sir.

Senator COBURN. Putting in the contract what you expect of the contractors to supply, which is certified people doing their jobs.

General PATTERSON. And many of the contractors do have an automated process. However, from time to time we do find discrepancies in their recordkeeping.

Senator COBURN. Good. So then you would fire that contractor, and that is what you put in the contract as a reason for you to lose the contract, and oh, by the way, we will have somebody else to have this contract next time.

General PATTERSON. Yes, sir.

Senator COBURN. These are not non-lucrative contracts. They are making money off of every hour every guard works.

Chairman CARPER. I want to——

Senator COBURN. I ask unanimous consent that this be made part of the record.

Chairman CARPER. Without objection, this letter[1] will be made part of the record.

Chairman CARPER. I want to pivot a little bit here and just say as a defense contractor with a valid Department of Defense ID card, Aaron Alexis was allowed access to the Washington Navy Yard, as we know. And like many employees in other workplaces, he was considered a trusted employee, not screened for any weapons. Unfortunately, workplace violence continues to be a threat.

I just want to start with you, Mr. Lewis, if I could here, but could each of you answer really the following two questions? The first question is: Do you believe that we should consider screening employees as well as visitors at Federal facilities?

Second, is there any potential downside to screening employees? And I would like for each of you to answer that. Mr. Lewis, if you would start first.

Mr. LEWIS. Current DOD policy does not require that type of screening where someone goes through a metal detection device. But it does allow for random selection of individuals for that type of screening. So there are procedures in place, there is the option in place, and again, we rely on the judgment of the installation commander to make a determination as to what is appropriate under the local circumstances.

The drawback to screening every employee coming through is the negative impact on mission accomplishment, and there are facilities where there are 10,000 employees coming through often in roughly the same window, and screening every single employee would be disruptive to getting the work done. And that is the balance, factoring in cost and mission accomplishment against screening every employee.

Chairman CARPER. All right. Thank you.

Mr. Patterson.

General PATTERSON. Yes, sir. I think it is something I am sure can be considered. We put a lot of trust in the system that we have. We put a lot of trust in the fact that we do background investiga-

[1] The letter referenced by Senator Coburn appears in the Appendix on page 254.

tions, and once a background investigation is completed, we believe that the individual that has received that background investigation is trustworthy.

So if we decide that we do not believe in that background investigation, that may be the time we start looking at a system where we screen all of our employees as they come in. It is a way to begin to mitigate, some of the risk, but, again, I think it would be something that we would have to think through very carefully.

I know that in some of our facilities we have both. In the Department of Transportation (DOT), they screen everybody in their headquarters building. In other facilities, they only screen the visitors that come through. So to date, in most of our facilities we have not had a problem with our employees or with the folks who have been screened.

If we decide that we are going to screen, then it might be a bit of a challenge only because it is a new process, and that process will require a longer processing time for our folks to get through. So we would have to carefully work with GSA and others in how we organize that flow because at 8 o'clock in the morning when you have literally hundreds of people entering a building and when they are accustomed to just moving through and showing their badge based upon a security clearance, it could create a challenge.

Chairman CARPER. All right. Secretary Durkovich, same question, please.

Ms. DURKOVICH. So as I mentioned, the Interagency Security Committee has put some thought through at least how we go about screening visitors as they enter into our Federal facilities, and part of that is based again on the facility security level. I would agree with my colleague Director Patterson in that we have to have trust in the system. And at the Department of Homeland Security, in addition to evaluating who has clearances, we also ensure that employees and contractors who are affiliated with the Department also undergo a suitability determination.

I think in order to ensure that there is not a negative impact on the mission, and we have to account for the fact that there are resource implications but opportunity costs associated with screening employees that, I think the system that we have in place works overall. And unfortunately we do have incidents where I think it is incumbent on us to look at those incidents and to make sure that we are leveraging the lessons learned so we make sure that it does not happen again.

But I think that overall there is a downside to screening employees. As you know, sir, from your oversight of the Department, we all have taken on an awful lot of work to ensure the safety and security of the American people and that its way of life can thrive, and that any impediment or obstacle to allowing our employees to do their important job every day is an impact on the mission. And we have processes in place that allow us to ensure that we have employees who represent the highest standards and that we should continue to trust in that system as opposed to screening everyone.

Clearly, at certain facilities we do have measures in place, as Director Patterson recognized. When I got to the Nebraska Avenue Complex (NAC) every day I have to show—not only swipe my badge but show my badge. There is a physical ID. If I am bringing

a vehicle on to the premises, there are dogs and there are vehicle searches that happen. So there are, again, depending on the level of facility, different layers of security. But in terms of actually putting people through, no.

Chairman CARPER. OK. Thanks.

Before I recognize Senator Ayotte for any questions she might like to ask, let me just ask one last quick question, and I will ask you to be very brief.

Some of you have been before us before, and I like to ask so much of what you are expected to do and those who work for you are expected to do to meet your responsibilities. What can we do here, just maybe give me one good idea of what can we do in the legislative branch to better ensure that you are able to meet the responsibilities that have been placed on you for workplace protection.

And while you are thinking about that, I will just mention this. Today Senator Ayotte and I and our colleagues are debating a budget resolution, if you will, a framework for a spending plan for the Federal Government for the balance of this fiscal year. It does a number of things. I think there are three things we ought to do for deficit reduction, at least this makes it really simple:

No. 1, entitlement reform that saves money, saves the programs, does not savage old people or poor people;

No. 2, tax reform that eliminates a number of our tax expenditures. We have a lot of them, some of which have met their purpose, have long met their purpose, and they need to be retired or modified. But use some of the revenues that we generate to reduce corporate tax rates and use some of the revenues for deficit reduction;

No. 3, just look at everything we do and say across the Federal Government how do we get better results for less money for everything we do.

Those are three things that I continue to harp on, but one of the things that we do with the budget resolution, if you will, an omnibus appropriations bill, or separate appropriations bills that follow, is that we move away a little bit from sequestration, across-the-board cuts, to allow agencies and departments to better say this is the way we need to allocate resources. Hopefully that is something that will enable us to look at risk, look at areas of risk, put more money there, and areas of less risk, because able to put less money there. But in terms of what we can do to help you do your work better, each of you just give us one good idea, and just be very brief.

Ms. DURKOVICH. I will start, and in some ways, sir, you have answered my question, or you have given my response, and it is recognizing that in this country there are a number of risks that we face. It is a large country, and part of the conversation that we have to have as both the Department of Homeland Security, as an administration, as law makers, and with the American public is we cannot mitigate every threat. And so it is our understanding that those are going to have the most significant consequences and ensuring that we are having a conversation about how we go about mitigating them, that we have the resources, the personnel to go

about doing that. So having the conversations that we have today and over the course of time is I think what is critical.

You have already taken steps by moving away from sequestration. That will be helpful to us as well. But, again, I think that recognizing that we have to manage risk and that we cannot prevent every incident, and as long as we are adapting, that is what is key.

Chairman CARPER. OK. Thank you. General.

General PATTERSON. Yes, sir. The Federal Protective Service is in——

Chairman CARPER. I am going to ask you to be very brief.

General PATTERSON. Yes, sir FPS is—in a fairly unique position in that we have to work and weave our way through both State, local, Federal, and civilian contractor environments, and we do that with a very small force. Your support in helping us to move through and navigate through some of those areas is critical, because we are trying to look out and predict, what is coming down the road to keep our people safe, and we really need the support of folks like yourself and this Committee to help us work through some of these challenges.

Chairman CARPER. All right. Thank you.

Mr. Lewis, same question. A very brief response, please.

Mr. LEWIS. We believe that continuing to evaluate those employees who have access to classified information and to our facilities is critical, and we need to have the resources to be able to conduct those evaluations, and we need to have access to records that are sometimes publicly available, sometimes not publicly available, in order to do those evaluations. And general support for that approach to doing business I think is essential.

Chairman CARPER. All right. Thanks. Thanks so much.

Senator Ayotte, welcome. Before you arrived, I was saying to Senator Heitkamp who was here that we are blessed in this Committee to have not one, not two, not three—we used to have four with Jeff Chiesa—Attorney Generals, former State Attorney Generals on this Committee that really add a great deal of expertise in this particular area. So welcome.

Senator AYOTTE. Well, thank you, Mr. Chairman. I want to thank the witnesses for being here.

I wanted to followup with you, Mr. Lewis, and ask you about how other DOD policies might affect the security clearances at facilities and then those who can gain access to them, in particular, just a thought of whether there are any DOD regulations that need to be reviewed or revised, for example, the current discharge regulations and how they are implemented.

As I understand it, in the case of Mr. Alexis, had he been dishonorably discharged, that would have raised a flag, and that obviously would have gone right directly to his fitness to hold the security clearance.

Could you help me understand, in light of this case, is this something that we need to think about? And one of the things that I am wondering about as well is the whole breakdown with the reach-out. Obviously that was beyond—but is there anything that we need to do on the mental health end here looking back on this? And I understand that 20/20—it is always 20/20 when you look back at something and you can see things that you did not see at

the time. But what I am trying to understand, is there anything that we need to look at internally on those two issues from the DOD perspective or anything we can do—I also serve on the Armed Services Committee—working jointly, the committees, that we should be doing?

Mr. LEWIS. I do not believe that there are issues with how the discharges occur, and not to get into specifics, but generally based on what was known at the time of the discharge, it was not considered to be an unusual determination as to an honorable discharge in that particular case.

But the larger issue is how do we collect—how do we identify and collect relevant information that allows us to constantly adjust our perspective about cleared individuals and individuals who are in trusted positions? And that is really the challenge.

I hate to keep blowing the same horn, but the continuous evaluation process of not just collecting the information but having the staff available to evaluate the information and take action on that information, to me that is the real issue here.

Senator AYOTTE. Well, I appreciate it. Then, of course, Senator Collins, Senator McCaskill, Senator Heitkamp, and I also have one where there would be random checks that I think is important as well, after you receive your security clearance. It is a pretty lengthy period right now upon which there is a review unless there is a reason that something is flagged.

I wanted to ask also, General Patterson, what do you see as we look at this whole situation now with what is happening at the Navy Yard that you are already implementing to make sure that we do not find ourselves in the same situation? We can obviously legislate, but I know you are reviewing the whole situation and understanding what steps you are already taking in a positive fashion that you can talk about here?

General PATTERSON. Yes, ma'am. Within the Federal Protective Service, we are working very closely with our Federal partners to look at processes and procedures for folks coming and going into Federal buildings. But we are also looking at our communications processes as well. One of the challenges during the Navy Yard was just the fact that so many agencies responded, just the level of communication and how do you do that. And so we are looking aggressively at how we do that, not just in the Washington, DC, area but across the United States, because in a crisis situation, communication becomes critical, and as such, good, timely communications is essential, hopefully, to a positive result.

So we are looking in a variety of areas and taking lessons from the Navy Yard as to how we improve processes across the spectrum within the Federal Protective Service.

Senator AYOTTE. Thank you very much.

I also wanted to ask you, General Patterson, is it accurate to say that FPS does not use a risk assessment tool consistent with the Interagency Security Committee's standards? I am trying to understand where we are with this, and I know that there was also a report from GAO that FPS' interim facility assessment tool was not consistent with the assessment standards because it excludes consequence from assessments. And I want to understand if there is

a difference, why is it there? Is it something that we should be more uniformly putting in place? Or is there a reason for it?

General PATTERSON. There is a reason, and we have just built the Modified Infrastructure Survey Tool (MIST), and that particular tool was developed with the Infrastructure Protection folks, within the Department who had developed a tool over a period of about 6 or 7 years. And we thought that this was a tool that we could modify because it brought what we believe are all of the areas of the ISC requirements to bear.

Now, with our tool we look at specifically vulnerability. That is what the tool is structured for, to look at the vulnerability of a facility. Separate from the vulnerability piece, we also do a threat assessment. We connect with the Joint Terrorism Task Force (JTTF), with local law enforcement, with any number of agencies out there to get what we believe is a very in-depth, comprehensive perspective on the threat that we also provide to our Federal partners.

The piece that is not part of the process is the consequence piece, and it is not part of that process because we have not figured out how to do that yet within a Federal facility.

Senator AYOTTE. What does that mean? Just so we understand.

General PATTERSON. Well, that is one of the things we are working with the ISC to help us better define. When you are asking for a consequence within the Federal sector, what is it you are looking for?

We know that when we help a Federal partner to begin to pull together and understand their emergency occupancy plans, we help them to understand and we go through the consequence piece, and when they are looking at establishing the facility security level, we are also looking at the consequence piece there. We have not figured out yet how to incorporate that in an automatic method that will allow us to provide a reasonable and rational meaning to consequence to, let us say, 10 tenants of a leased facility. We are fairly certain that folks like the IRS and Social Security and others have stepped through the consequences of losing a facility in the event something happened to the facility. But we have not figured out yet how to incorporate that into a tool, and that is something we are working with the ISC to figure that out.

Senator AYOTTE. OK. I appreciate your answer, and I want to thank all of you. We look forward to working with you on this important issue. Thank you.

Chairman CARPER. Thank you, Senator Ayotte.

At this point I am going to excuse this first panel of witnesses and thank you again for being here. Thanks for the work you are doing.

I would just say as you head back for work from here, just keep in mind all those people, the hundreds of families who lost loved ones in Oklahoma City in that bombing. Keep in mind those at Fort Hood who lost their loved ones. Keep in mind, if you will, the families of the 12 men and women who died at the Washington Navy Yard. And just think of them as they celebrate Christmas or some other holidays, the families sitting around the Christmas tree, their dining room table, and there is somebody missing.

We need to do our dead level best every day to ensure that those number of empty chairs, people that are not around because of a

tragedy like the ones I have just mentioned, keep them in mind, keep their families in mind and let that just energize our efforts going forward. This is not just about process. This is not just about GAO recommendations and complying with those recommendations. This is about saving people's lives and making sure they have a good life and a chance to share that life for a long time with their families. Take that with you. Thank you. [Pause.]

To our second and final panel, welcome. We are glad you could join us. Let me just very briefly introduce you, and then we will welcome your statements and have a chance to ask some questions.

Our first witness is Mark Goldstein. Mark is the Director of Physical Infrastructure Issues for the U.S. Government Accountability Office, as we mentioned earlier, is the investigative audit arm of the U.S. Congress. We are grateful for the work that you and your colleagues do. Mr. Goldstein is responsible for GAO's work in the area of government property, critical infrastructure, and telecommunications.

At the request of this Committee and I think other congressional committees, GAO has conducted 12 reviews of Federal facility security since the Federal Protective Service became part of the Department of Homeland Security in 2003. GAO reports have focused on oversight of contract guards, facility risk assessments, cooperation with local law enforcement, planning and budgeting for security, and challenges hampering the protection of Federal agencies.

Our second witness is Stephen Amitay. Is the emphasis on the first syllable?

Mr. AMITAY. Yes.

Chairman CARPER. Oh, good. Amitay. Stephen Amitay, Executive Director and General Counsel for the National Association of Security Companies. Mr. Amitay has led the association's efforts working with Congress, with Federal agencies, and the Government Accountability Office on programs, on legislation, and other issues related to facility security since 2006.

Our final witness is David Wright. Mr. Wright is the President of the National Protection and Programs Directorate Union, American Federation of Government Employees. Mr. Wright has served in his present capacity I believe since 2006, and Mr. Wright is a 27-year veteran of the Federal Protective Service. His last 12 years he served as an Inspector, performed myriad responsibilities necessary to that position, from responding to crimes to overseeing contract guards to performing facility security assessments. Mr. Wright brings a wealth of field experience before this Committee, and he has worked with the agency and Congress to find solutions to many of the challenges that face the Federal Protective Service. We thank you for all of that.

We welcome you all. You will each be invited to summarize your prepared statement. We would ask you to take about 5 minutes, and your entire statement will be made part of the record, as I indicated to the first panel. So thank you for joining us today.

Well, let me ask a question. Here is the first question: Were you all here for the first panel? Raise your hand. Ah, good. OK. That is great. Thanks. Thanks for staying for yours.

All right. You are recognized, Mr. Goldstein.

**TESTIMONY OF MARK L. GOLDSTEIN,[1] DIRECTOR, PHYSICAL INFRASTRUCTURE ISSUES, U.S. GOVERNMENT ACCOUNTABILITY OFFICE**

Mr. GOLDSTEIN. Thank you, Mr. Chairman and Members of the Committee. Thank you for the opportunity to testify this morning on issues related to the Federal Protective Service and the protection of Federal buildings.

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

My testimony this morning discusses challenges that FPS faces in, first, ensuring contract guards are deployed to Federal facilities and properly trained; and, second, conducting risk assessments at Federal facilities. It is based on GAO's work issued from 2008 through 2013 on FPS' contract guard and risk assessment programs and preliminary results of GAO's ongoing work to determine the extent to which FPS and select Federal agency facility risk assessment methodologies align with Federal risk assessment standards. Our findings are as follows:

First, FPS faces challenges ensuring that contract guards have been properly trained and certified before being deployed to Federal facilities around the country. In our September 2013 report, we found that providing active-shooter response and screener training is a challenge for FPS.

For example, according to guard companies, at five guard companies, their contract guards have not received training in how to respond during incidents involving an active shooter. Without ensuring that all guards receive training in how to respond to incidents at Federal facilities involving an active shooter, FPS has limited assurance that its guards are prepared for this threat.

Similarly, an official from one of FPS' contract guard companies stated that 133, about 38 percent, of its 350 guards have never received screener training. As a result, guards deployed to Federal facilities may be using X-ray and magnetometer equipment that they are not qualified to use, which raises questions about their ability to screen access control points at Federal facilities—one of their primary responsibilities.

GAO was unable to determine the extent to which FPS' guards have received active-shooter response and screener training in part because FPS lacks a comprehensive and reliable system for guard oversight. FPS agreed with GAO's 2013 recommendation that they take steps to identify guards that have not received 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 our 2012

[1] The prepared statement of Mr. Goldstein appears in the Appendix on page 210.

recommendation that it develop a comprehensive and reliable system for managing information on guards' training, certifications, and qualifications, it does not yet have such a system.

Second, FPS also continues to face challenges assessing risk at Federal facilities. GAO reported in 2012 that FPS is not assessing risk at Federal facilities in a manner consistent with Federal standards. GAO's preliminary results from its ongoing work on risk assessments at Federal facilities indicates that it still is a challenge for FPS and several other Federal facilities.

Federal standards, such as the National Infrastructure Protection Plan's risk management framework and ISC's risk assessment provisions, state that a risk assessment should include threat, vulnerability, and consequence assessments. Risk assessments help decisionmakers to identify and evaluate security risks and implement protective measures to mitigate that risk. Instead of conducting risk assessments, FPS is using an interim vulnerability assessment tool, referred to as the Modified Infrastructure Survey Tool to assess Federal facilities until it develops a longer-term solution. However, MIST does not assess the consequence—the level, duration, and nature of potential loss resulting from an undesirable event. Risk assessment experts GAO spoke with generally agreed that a tool that does not estimate consequences does not allow an agency to fully assess its risks. Thus, FPS has limited knowledge of risks faced at about 9,600 Federal facilities around the country. FPS officials stated that they did not include consequence information in MIST because it was not part of the original design. GAO will continue to monitor this issue and plans to issue a report on this issue early next year.

In response to our recent reports, DHS and FPS have agreed with the recommendations in our 2012 and 2013 reports to improve FPS contract guard and the risk assessment processes.

Mr. Chairman, this concludes my opening statement. I will be happy to answer questions you may have. Thank you.

Chairman CARPER. Good. Thanks so much, Mr. Goldstein.

Mr. Amitay, please.

**TESTIMONY OF STEPHEN D. AMITAY,[1] EXECUTIVE DIRECTOR, NATIONAL ASSOCIATION OF SECURITY COMPANIES**

Mr. AMITAY. Chairman Carper, Senator Ayotte, my name is Stephen Amitay, and I am Executive Director for the National Association of Security Companies. NASCO is the Nation's largest contract security trade association whose member companies employ more than 300,000 security officers across the Nation servicing commercial and governmental clients, including numerous Federal agencies. NASCO works with legislators and officials at every level of government to put in place higher standards and requirements for security companies and private security officers.

Of most relevance to today's hearing, since 2007 NASCO has worked with Congress, FPS, and GAO on issues and legislation related to the Federal Protective Service's Protective Security Officer Program. It was formerly called the Contract Guard Program. NASCO also worked with the Federal Interagency Security Com-

[1] The prepared statement of Mr. Amitay appears in the Appendix on page 221.

mittee on its 2013 best practices for armed security officers in Federal facilities.

Not including the military services, there are approximately 35,000 contract security officers across the Federal Government, and the use of contract security is a proven, effective, and cost-efficient countermeasure to reduce risk and mitigate threats to Federal facilities.

To further ensure security at Federal facilities, FPS and its security contractors need to work together to address issues and challenges with the PSO program that GAO has identified over the past several years. At the same time, improvements need to be made to other elements in the risk assessment and threat mitigation process for Federal facilities. These elements are governed by ISC standards; however, as GSA has found out and as we learned earlier today, often the requirements of the ISC standards are not met by Federal facilities.

One critical element in this process is the decision to implement specific security countermeasures for each facility. In GSA-owned or—leased buildings, FPS is responsible for conducting the facility security assessment and recommending countermeasures. But, Mr. Chairman, as you noted in your opening remarks, the decision to implement those recommendations or, put another way, the decision to mitigate risk or accept risk is solely up to the Facility Security Committee, which is made up of representatives from facilities' tenant agencies.

However, again, as GAO has found, "tenant agency representatives to the FSC generally do not have any security knowledge or experience but are expected to make security decisions for their respective agencies." The lack of experienced decisionmakers on FSC is something that security contractors have witnessed firsthand, and it calls into question whether FSCs are making informed risk-based decisions regarding the mitigation or acceptance of risk.

Of course, tightened budgets have also put pressure on tenant agencies to accept more risk. In the end, though, countermeasures deemed necessary for security should not be rejected because of either lack of understanding or an unwillingness to provide funding.

NASCO supports requiring training for FSC members as well as DHS being able to challenge an FSC over noncompliance with ISC standards or decision not to implement countermeasures. Both these provisions were in legislation that was passed last Congress by this Committee.

As to addressing the issues with FPS' PSO program that GAO has identified, as well as other issues with the program, while FPS' pace may not be as fast as GSA and security contractors would like, nonetheless FPS' commitment to improving the PSO program is unquestionable, and there has been substantial progress made.

Since the appointment of Director Patterson, the degree of dialogue and breadth of cooperation between FPS and security contractors has been unparalleled, and currently FPS and security contractors are working on a host of initiatives to improve the PSO program.

To address the lack of FPS personnel resources to provide critical PSO X-ray and magnetometer training, FPS is about to launch a pilot program developed with NASCO that will train and certify

contractor instructors so that they can provide this important training. FPS is also moving to increase active-shooter training for PSOs and, wisely, they are looking at what other Federal agencies are doing in this area as well as seeking input from security contractors.

FPS is working with NASCO to revise and standardize the PSO training lesson plans and is planning to require that security contractor instructors be certified for all areas of PSO training.

FPS is also coming out with a much needed revision of the Security Guard Information Manual (SGIM). The SGIM governs and instructs PSOs on how to act, and not following the SGIM is considered a contract violation. The format of this new version will also allow for making revisions as needed.

One area that needs further review are the instructions related to a PSO's ability and authority to act and potential liability for acting in extreme situations such as active shooters. As is provided to contract security officers at some other Federal agencies, Congress might want to consider providing DHS with statutory authority to authorize PSOs to make arrests on Federal property.

FPS is also working to improve PSO post orders and improve its management of PSO training and certification data. For this latter effort, NASCO strongly recommends that FPS explore commercially available technologies.

In conclusion, much still needs to be done to address the PSO program issues raised by GAO. However, FPS has come a long way in the past decade with its contract security force. NASCO looks forward to continuing to work with FPS and Congress to improve the security at Federal facilities.

Thank you.

Chairman CARPER. Mr. Amitay, thank you so much.

Mr. Wright, you are now recognized.

**TESTIMONY OF DAVID L. WRIGHT,[1] PRESIDENT, FEDERAL PROTECTIVE SERVICE UNION, AMERICAN FEDERATION OF GOVERNMENT EMPLOYEES**

Mr. WRIGHT. Chairman Carper, Senator Ayotte, thank you for the opportunity to testify at this important hearing. I am David Wright, President of American Federation of Government Employees (AFGE) Local 918, which represents Federal Protective Service officers nationwide. I am also an inspector with the FPS. We are committed to the critical homeland security mission of securing our Nation's Federal buildings, but there are important issues that require resolution.

Federal employees and facilities are extremely vulnerable to attack from both criminal and terrorist threats. I want to assure you that my fellow FPS law enforcement officers are trained, equipped, and competent at responding to active-shooter attacks, and I am appalled that bureaucracy and inefficiency restricted our FPS law enforcement officers, whose office is less than 1 mile away from the Navy Yard, from assisting with the pursuit of the active shooter. Basically it is because the Navy does not pay security fees to the FPS.

[1] The prepared statement of Mr. Wright appears in the Appendix on page 239.

Congressional review of physical security at Federal properties must be viewed in the context of the leadership required to accomplish the FPS mission, which, to say the least, remains unfocused, if not broken, at all levels. Physical security plays a significant role in protection of all occupants of Federal buildings, but the frustrating, inefficient, and outright wasteful bureaucratic system of implementing physical security countermeasures through a flawed facility security assessment process and implementation by facility security committees who have to divert their mission funding is eye candy and not true security. Security in the Dirksen Senate Office Building is not based on an individual Senate office's ability to pay. Why should other major Federal facilities be different?

The FPS inspector workforce is constantly beleaguered by new and/or modified security assessment programs and individual conflicting management demands throughout the assessment process. I have lost confidence in the ability of the National Protection Programs Directorate to resolve this wasteful process.

I understand that the Department's Science and Technology Directorate has offered to make the integrated rapid visual screening tool compliant with the ISC. It was tested by both the General Services Administration and officials at the Federal Protective Service. I think that would be a good start to remedying our assessment problems.

Use of private contract security guards at major Federal facilities is a risk because they are basically limited to the arrest powers of a citizen. The proactive law enforcement patrol and weapons screening at this building is accomplished by Federal police officers who have the lawful authority to respond to active shooters. How can we demand less in Federal buildings with thousands of occupants?

How well are the 740 or so boots-on-the-ground officers and agents doing—providing the critical law enforcement protection of Federal buildings overall quite well given the dynamic mission, the headquarters staff with very little field experience, and an inadequate field staff? How is FPS management doing? Not so well. Can do better? Absolutely. Any organization is in trouble when leaders are not held accountable. A recent Office of Special Counsel (OSC) public file disclosure reveals that a regional director violated rules when he arranged to buy a system from his neighbor on behalf of the government. The punishment of a 3-day suspension is the opposite of accountability. I have been told that there are other instances of misconduct by equal and even higher-ranking officials.

After accountability is established, performance across the board can improve with focused professional and ethical management that builds on best practices in the regions. Give our inspectors and police officers adequate staff, tools that work, and direction on priorities, and we will make sure the job is done.

In conclusion, the Federal employees and the public they serve deserve the best and most effective protection we can provide. They are not getting it now, and expeditious, sincere action by DHS and Congress is required. Once again, I thank you for this opportunity, and I am available for questions.

Chairman CARPER. Great. Mr. Wright, thanks very much for coming and for your service.

I am going to yield to Senator Ayotte for the first questions of this panel. Senator Ayotte.

Senator AYOTTE. Thank you very much, Mr. Chairman. I really appreciate that.

I wanted to ask Mr. Goldstein if—particularly on the GAO reports and what you have found, it really troubles me when we think about that there is no comprehensive—I believe you described it as strategy or oversight model, and then the fact that we are not sure how many people are receiving—there is certainly a category that are not receiving active-shooter training and/or screener training.

From the GAO perspective what is your recommendation in terms of from the policy perspective how we can move this as quickly as possible to address this problem?

Mr. GOLDSTEIN. Thank you, Senator. We have been very concerned that, with respect to both active-shooter training and training on magnetometers, FPS has not done a good enough job at ensuring that its contract guard workforce is able to get that training.

One of the problems with the active-shooter training which I think people do not understand here, though, is that it is only a very small part of just one part of the training they receive anyhow. They get a kind of special training of 2 hours which covers special events of various kinds that might occur in a building. So out of the 120 hours of training that they receive overall, only 2 hours go to special events, and only a fraction of that 2 hours actually covers active-shooter training.

So I think it is important to recognize that, for all intents and purposes, contract guards are not really getting active-shooter training for the most part. We are concerned that they do not have enough training in this area.

The same is true for magnetometers. When GAO did its penetration testing of a number of Federal buildings back in 2009 and penetrated all 10 buildings that we tried to get into in a variety of different cities with bomb-making materials, we found at that time that guards did not have the requisite training to be at post, and we find now several years later that many guards still do not have that training.

Senator AYOTTE. And these are the contract guards, correct?

Mr. GOLDSTEIN. Yes, ma'am.

Senator AYOTTE. So let me ask Mr. Wright, with respect to the agencies that can pay the fee, how does your training differ? How did the training of the individuals that I understand would work—and maybe I have this wrong, but would work in the Federal Protective Service Union when we are looking at this training issue, do you know how the training differs?

Mr. WRIGHT. As Federal law enforcement officers, we complete our training at the Federal Law Enforcement Training Center——

Senator AYOTTE. So you would go through the same training as any Federal law enforcement officer?

Mr. WRIGHT. Yes.

Senator AYOTTE. OK.

Mr. WRIGHT. And there is a slight difference. We are talking contract guards. They are stationary at their post; whereas, our Federal Protective Service inspectors and police officers are mobile.

Senator AYOTTE. To the point of your testimony, if you were to provide the services, for example, at the Navy Yard that the Federal Protective Service—just so I understand, would you do more of a roaming capacity, is what you are saying? You would not do the person who stands—because the Capitol Police officers here, they actually stand at the magnetometer when we walk through, and I am just trying to understand physically what this would look like.

Mr. WRIGHT. Right, and I think that is the model that I would look for, is a model that works here at the Capitol and the Capitol buildings, that you would have Federal officers begin their career at the magnetometer, at the X-rays before they promote up and gain seniority and go out into the field.

Senator AYOTTE. And I want to understand, are there other agencies that, with regard to this training issue on the FPS contracting issue, is this something that we are facing beyond the Navy Yard? I mean, I assume that this contracting issue in terms of the training issue goes well beyond the Navy Yard facility. Is that true, Mr. Goldstein?

Mr. GOLDSTEIN. The work we have done here really focuses on FPS, so I cannot comment more broadly. We have not looked at contract guard situations and what training they maybe——

Senator AYOTTE. So it would really just be focused here on the Navy Yard.

Mr. GOLDSTEIN. Right, but we have found that the kind of training overall that FPS gives its contract guards, is similar to training given by DOE, by the National Aeronautics and Space Administration (NASA), by the Pentagon Force Protection Agency, State, Kennedy Center. So they are in line generally with the kinds of training that you would give to a contract guard at a Federal facility. The problem is implementing it. That is where we seem to see the fall-off, ensuring that the guards are actually getting that training.

Senator AYOTTE. So there is basically no accountability. In other words, we can check off the training box, but no one is saying this person actually has done it, that we are tracking them. I mean, basically in a law enforcement setting, you have to do a certain amount of training that you have to complete every year, and that is part of being in that position. That is not happening with this?

Mr. AMITAY. Well, excuse me. As Senator Coburn noted, those are contract requirements to have your protective security officers have the required training and certifications, and that would be a contract violation. So, you know——

Senator AYOTTE. So we are actually entering contracts where we do not have them required to train on screening and——

Mr. AMITAY. The requirements are in the contract.

Senator AYOTTE [continuing]. Active shooters?

Mr. AMITAY. With the X-ray and magnetometer training, that—of the 132 hours of required training for FPS protective security officers, the contract guards, 16 hours are provided by FPS, 8 of which is X-ray/mag screening. And FPS' inability for their personnel to be able to provide that training is an issue that the GAO has noted. But that is not a matter of the security contractors not providing the training that they are required to provide.

Senator AYOTTE. So we are not providing the training for the security contractors, but we should be reviewing these contracts to make sure that we are properly prioritizing what type of agreement we are brokering in terms of the requirements for background and training, shouldn't we?

Mr. GOLDSTEIN. Yes, there are a couple of issues. One is, as Mr. Amitay says correctly, that the Federal Protective Service is not providing in many cases the training that they are obligated to provide under the contract.

Senator AYOTTE. Right.

Mr. GOLDSTEIN. On the other hand, FPS is also not gaining the assurance that it needs that the contract guard companies themselves are providing the training that they are obligated to provide. They are not doing enough checks on the certifications.

Senator AYOTTE. And who is watching all this? I mean, isn't there supposed to be——

Mr. GOLDSTEIN. I guess GAO——

Senator AYOTTE. But, I mean, you are watching it, but who within the chain of command, meaning the management of this, is making sure that it gets done?

Mr. GOLDSTEIN. Each region is supposed to go through a process to assure themselves and do checks and do audits. Some regions have not done it. Some regions have not done it in a random fashion at all where they could really gain assurance. Some have done it. When we have gone in behind them and looked at what they have done, not only did we find our own breaches in many cases of guards standing post without the proper certifications and qualifications; we also found significant disparities between our review and the review that FPS had done as well.

Mr. AMITAY. I also think some of those disparities are disparities in the documentation per se, and I think there are instances where the guards have received the required training, they do have the required certifications, but there are issues with the documentation.

For instance, with certain medical requirements, some statements of work require a licensed physician to sign off on those medical requirements. On others it could be a nurse practitioner. And GAO might come in and looking at what the current requirements are for licensed physicians and see that, oh, this PSO was signed off by a nurse practitioner; therefore, that is in violation.

Senator AYOTTE. Well, I know my time is up, but what we are talking about here, though, is the documentation on the training for, I assume, the most important focus here, the screening and active-shooter training.

Mr. GOLDSTEIN. It was a wide variety of issues. We found not just the magnetometer and the active-shooter training, but we found 23 percent of files we reviewed contained no documentation for required training and certification in a variety of areas. This could be firearms training, or drug testing, and there was no indication that FPS had monitored firearms qualifications in 68 of the files we reviewed. So it is across the spectrum of the kinds of certifications guards need.

Senator AYOTTE. Well, my time is up, so I will thank you.

Chairman CARPER. Thank you. Thank you for those questions.

I am going to ask two questions. The second question I am going to ask is when—in some sense, I like to ask when we are in a situation like this—a couple different panels, different points of view, a broad range of perspectives from which to testify and answer questions. I want you to each pick maybe one—or we will say two—go back to what you have heard one another saying in response to—well, it could just be your testimony, your response to our questions. Think back to the first panel, some of the things that they said, things they said in the testimony or in response to our questions, and just be thinking about takeaways for us on this side of the dais that you would just like to put an exclamation point behind, underline, and say as we go out of this room today, this hearing room, for God's sake, keep these couple of points in mind, these are really good takeaways. And that is my second question, so you can be thinking about that.

The first question I have is for Mr. Goldstein, and we have already talked about this to some extent. I am going to come back and just revisit it very briefly. But in the past decade or so, you have overseen, I think, 12 independent reports of Federal facility security. You have looked at the armed guard programs. You have collaborated with State and local law enforcement in human capital planning. GAO has also conducted covert testing. You have talked a little bit about some of what is going on in Federal facilities. In other words, you actually tried to penetrate Federal facilities to test how secure they are, which is a little bit like what we do in the nuclear power plant world.

Again, for the record, how would you assess Federal facility security today? Over 30,000 feet, how would you assess Federal facility security today, realizing this is on a time continuum, where we focus more and more on this going back to especially 1995 with the bombing in Oklahoma City? But how are we doing today? Is it getting better? Is it getting worse? Have we plateaued? Is it uneven?

Mr. GOLDSTEIN. I think it is very uneven, Mr. Chairman. I think that, yes, there have been improvements since Oklahoma City and since the Twin Towers, of course. We have more focus on this area. We have more physical protections in many places. We have more intelligence as well. But some of the basic issues still remain unresolved, the kinds of issues that you have brought up and that some of your witnesses have brought up this morning. There is still inadequate attention to many of the things that are in the forefront of what we need to do in terms of getting into a Federal building and making sure not only that the people who stand on the front lines of Federal buildings are qualified to be there and can do the service that they are being paid to do, that taxpayers are paying them for; but more broadly that we are wisely using government resources in this area.

Because we have not effectively adapted a risk management process to the Federal portfolio, virtually every building that is at a Level 3 or a Level 4 security risk is treated in the same fashion, and we do not prioritize across that portfolio in an effective way to make sure that we are effectively spending government resources. So I think we still have a long way to go, sir.

Chairman CARPER. All right. A followup question. If you maybe had to pick the next thing that the Federal Protective Service

ought to be doing in order to further improve Federal facility security as expeditiously as possible—and I do not know if that is a fair question, but take a shot at it.

Mr. GOLDSTEIN. Sure. I mean, we have talked a lot this morning about the two fundamental issues in our last report on risk assessments and on contract guards. And while they are moving slowly, I think they are trying to move in the right direction in both of those areas.

I think the area that still bedevils the security community here and has come up a couple times is this three-legged stool between GSA, the facility Security Committees, and FPS, in trying to figure out the best way to get security at Federal buildings. Should there really be a very significant role for individual agencies within a specific building for people who do not have a lot of security background? Should they really be making decisions about the government's buildings?

I do think while the ISC has developed standards to try and improve the level and effectiveness of the Facility Security Committees, that is an area that I think they still need to spend a lot more time in trying to figure out—is that really the best way that we can protect Federal buildings.

Chairman CARPER. OK. Good. Thank you very much.

All right. Mr. Wright, I am going to ask you to respond to my first question. Again, a point or two that you would really like to say, for God's sake, if you forget everything else that you heard in this hearing, do not forget this. And there is probably more than a few things that we ought to keep in mind, and we will, but just one or two if you would.

Mr. WRIGHT. If you will indulge, the focus of this hearing was the Navy Yard tragedy, so just very clearly, right off the bat, in regards to active shooter, look at our jurisdiction and authority. Our guys responded to the Navy Yard. We were less than 2 minutes away, and we had people at the Department of Transportation facility right across the street ready to activate and use their training and equipment, and we were held back. So that is just real, low-level stuff.

I need you to demand accountability. This Committee, as referred to by Mr. Goldstein, in 2009 after they penetrated 10 of our buildings, our FPS Director sat here and committed to this Committee that he would fix the National Weapons Detection Training Program. To this day, that program is not complete.

Chairman CARPER. Are we making any progress?

Mr. WRIGHT. Uneven. It is scattered across the Nation. I think one of the big problems with FPS is you finally have a vision or at least somewhat of a vision at headquarters, and I guarantee you, once that vision leaves headquarters, it goes down to 11 different regions, I think three, four, five different Senior Executive Service (SES) officials, and the message gets lost, thereby once again reducing any semblance of accountability. We have 11 different regions and 11 different ways of doing business regardless of what our headquarters says.

Chairman CARPER. OK. Thank you. Mr. Amitay.

Mr. AMITAY. Yes, thank you. Going off what David just said, it is true that there is a vision now at headquarters. Part of that vi-

sion is to standardize the training, to increase the training, and the lines of communications with the regions do need to be improved. And that has always been a problem, though, with FPS, is the fact that it has had to deal with 11 different regions.

I think, though, you will see at FPS—David also mentioned the National Weapons Detection Training Program, which is basically the X-ray and magnetometer training for PSOs. That is a new program that will require 16 hours of initial training and then 8 hours of annual refresher training. Compare that to the current requirement of 8 hours of initial training, and then, essentially 8 hours that is combined with 40 hours of refresher training every 3 years. That is a positive development. The delivery of this training, though, that has been a problem, and it has been slow getting it out. And I think FPS realizes that the stretched-thin FPS inspectors really should not be doing training. That should not be their mission. And they are starting to turn this over to the—they want to turn it over to certified contract security instructors, and we think that is a great idea. That will allow for more cost-efficient and faster training.

Also, in active-shooter training, definitely FPS needs to be doing more with that. I mean, other agencies are well ahead of FPS in terms of training their contract security officers to respond to active-shooter incidents. I have talked with several contractors, and they basically say that with those instructions and post orders, there really is some confusion for PSOs as to what they can do in an active-shooter situation.

I mean obviously, as the instructions do say, when you are faced with an active shooter and the loss of life, you can engage them. But, are they able to be more aggressive in terms of maybe detecting an active shooter? If a person comes in, is being really suspicious, can they kind of get into the guy's face and see what he is doing?

I have been told that at DOE the active-shooter policy for their contract security officers is basically do not let the threat continue, period.

But I think FPS is working to improve the training, to bring it up to a higher quality. They are working also, as Mark said, to try to better monitor their certification and training records, and, Mark, stay on them with that, because we do think that there is technology out there. I sometimes cringe when they say, well, we are working with the Science and Technology Directorate to basically try to come up with a data management system, something that, as Mr. Coburn pointed out, the contractors must have and already do have. And so there should be greater integration in terms of a comprehensive data management system, so the FPS and contractors can know and GAO can know who exactly does have the required training and certifications.

Chairman CARPER. All right. Thank you.

Mr. Goldstein, the last word.

Mr. GOLDSTEIN. Thank you, Mr. Chairman. One quick clarification for Dr. Coburn's benefit. Regarding GAO's recommendations, there have been 26 between 2010 and 2013. By our records, only four are in process, and have only been in process for about 3 or 4 weeks when we received them, meaning that there are 22 still

open. We will provide your staff with the exact information behind all those.

Chairman CARPER. Thank you. That is very interesting. Thank you for that clarification.

Mr. GOLDSTEIN. Yes, sir.

Just three brief points that have not been brought up too much this morning which I think are very relevant.

The first, as Mr. Amitay has said, I think it is important that there be better clarity in terms of contractors' liabilities. We have interviewed dozens and dozens of contract guards over the last decade, all of whom have felt that they do not have clarity on what their roles and responsibilities are and when they can use force and when they cannot use force. And most have told us over the years that their companies have all but said, "Don't you ever pull out your gun. Don't you ever do anything with it." So there is a lot of lack of clarity in this area.

The second is the role of the inspector at the Federal Protective Service. It would be great if they were able, as Mr. Wright has said, to roam around more, to do more things, to be able to assure the security of the buildings they are responsible for. But in many cases, they are locked at their desks. They are doing other work. They are involved in getting contracts out the door. They are often still contract officers. The level of things that they are responsible for really precludes them in many instances from actually being out and about and being the eyes and the ears and taking care of the police function that they really have. So that would be the second.

And then the third, finally, is I do not believe there really is much coordination at all based on the work we have done in the past with local and State police jurisdictions, so that when tragedy does strike that the Federal Protective Service has worked out in any kind of detail with local police jurisdictions exactly what kind of focus, what kind of approach, what kind of countermeasures they can take in the event of a tragedy. So more work needs to be done in that area as well.

Thank you, sir.

Chairman CARPER. Thank you. Thank you all for being here. Thank you for what you do with your lives. Thank you for your preparation for this hearing and for your responses to our questions.

Mr. Goldstein, a special thanks to everyone at GAO for the continued good work that you do.

Mr. GOLDSTEIN. Thank you, sir.

Chairman CARPER. I do not have time—the weekly caucus lunch has begun, and I am late. So I am going to wrap it up here. If we had more time, one of the things I would get into is the issue of turnover among these contract officers. I do not think we really spent much time on that. I would just say as a closing thought, when I was Governor of Delaware, we had a real problem in the area of information technology, training folks to work in that area for us as a State employee, developing their skills and getting hired away by someone who would pay them a lot more money. And the Governor who succeeded me was smart enough to realize that we

ought to pay and change up the way we rewarded and incentivized folks to work for the State of Delaware in that arena.

We have a similar problem actually here in the Federal Government. If you look at the skill sets and the compensation packages and the way we attract and retain skilled folks in the cyber world, in the Department of Homeland Security as compared, say, to the National Security Agency, there is a difference. And Dr. Coburn and I and our staffs and our colleagues are working on a way to reduce that disparity so that DHS will not just hire people to work in cybersecurity and see them trained and then hired away by others. We are going to work on that, and it would be interesting to know what we lose. Their training is so important here. That is one of the things we keep coming back to—the quality of the training, not just original training but refresher training, and the quality of that training.

The thought that is in the back of my mind is what is going on with turnover. My guess is there is a fair amount of that in these jobs, and so a lot of training that is done might not inure to the benefit of the Federal taxpayers, but to those who ultimately these contract officers go to work for.

If I had more time, I would ask each of you to respond to that, but if you would just raise your hands, and just by raising your hands, is that a problem? Is that a concern that we should have? OK. Thanks very much.

All right. I would just say in closing that the hearing record will remain open for the next 17 months—— [Laughter.]

Chairman CARPER. All right, 17 days, until January 3 at 5 p.m. for the submission of statements and questions for the record. I am sure you will get some, and we would appreciate your responding to those.

Again, thank you very much for being here with us today. Our best wishes to you and your families in this holiday season. Thanks very much.

[Whereupon, at 12:57 p.m., the Committee was adjourned.]

# APPENDIX

---

**Opening Statement of Chairman Thomas R. Carper**
**"The Navy Yard Tragedy: Examining Physical Security for Federal Facilities"**
**December 17, 2013**

*As prepared for delivery:*

Good morning and thank you for joining us today for this very important hearing that will take a closer look at physical security for federal facilities.

Three months ago, Aaron Alexis reported to the Washington Navy Yard with intentions to inflict pain and suffering on anyone in his path. We do not know now, and we probably never will be entirely clear why this tragedy came to pass, but hopefully, the lessons learned will provide a foundation for preventing future tragedies like this one.

Let's take a moment to recount how Aaron Alexis got the access to the Navy Yard that allowed him to successfully enter the facility that fateful morning.

In 2007, Aaron Alexis joined the U.S. Navy. As with other service members, a background check was performed and he was granted a low level security clearance. After an honorable discharge from the Navy in 2011, Alexis was hired by a defense contractor who confirmed he possessed a valid security clearance.

This marked him as a trustworthy individual. Because of that security clearance and that job, Alexis was provided with an I.D. card that would authorize his access to certain facilities, including Building 197 at the Washington Navy Yard.

Shortly before 8 a.m., on September 16, 2013, Aaron Alexis drove to the front gate of the Washington Navy Yard and displayed his access card. He was admitted by security, parked his car, and walked to Building 197.

Upon entering that building, Alexis encountered two additional security layers: an automated turnstile which required a valid access card and an armed security guard posted near an entrance.

Unfortunately, these measures were designed primarily to prevent unauthorized access and not to screen for weapons. Officials probably thought that the people working there were trustworthy because they had security clearances and had been vetted.

Eight minutes after Aaron Alexis cleared security he began shooting co-workers using a shotgun he had successfully concealed.

In the wake of the shooting at the Washington Navy Yard, this Committee began a review of security practices and procedures highlighted by the attack.

Our first oversight hearing looked at the security clearance processes that federal agencies have implemented to determine who should have access to sensitive information or facilities. At that hearing we explored ways to improve the process, and were reminded that quality cannot be

sacrificed for speed. The purpose of today's hearing is to review how we physically secure federal facilities from attack.

In many instances, security measures begin long before a person approaches the facility. Because Mr. Alexis was able to maintain a security clearance, he was trusted as a defense contractor and granted access to the Navy Yard complex. Aaron Alexis exploited this trust, and hurt innocent people.

In the aftermath, it is only natural that we wonder if all people entering a federal facility – even employees – should be screened in some way. Should we – to borrow a phrase from Ronald Reagan – "trust, but verify?"

Workplace violence and insider threats are just some of the examples of the many undesirable threats facing our federal facilities. There are many other potential threats that agencies must attempt to detect and deter. In addition to active shooters, agencies must develop countermeasures for improved explosive devices, biological weapons, and other types of assaults.

Today's hearing will examine federal agencies' efforts to develop and maintain effective layers of security at their facilities and prevent future attacks on innocent people.

Facility security is not just about protecting the physical structure of a building, it is about safeguarding the millions of innocent people who work and visit these facilities on a daily basis. Today's hearing on facility security is also about honoring the memory of the twelve men and women who died on September 16, 2013, by learning from that incident and doing all that we can to prevent a similar tragedy from happening again.

People who know me know I like to say, "If something is not perfect, make it better." My goal today is to figure out how we can do a better job protecting people at our federal facilities. We can start by asking some fundamental questions.

First, we need to ask: How do federal agencies determine what the threats are to their specific facilities?

Not every facility is the same. Large federal buildings in big cities – for example, the Alfred P. Murrah building in Oklahoma City – may be a target for terrorists because of their size and symbolism. However, the more likely threat to a small Social Security Administration office or an IRS Taxpayer Assistance Center is a tired or angry citizen reacting poorly out of impulse.

Second, we should ask: Are federal agencies properly assessing and prioritizing these threats?

I also frequently say, "The road to improvement is always under construction." The world around us is constantly changing. We should always try to figure out how to respond to that and do things better. I also think the methods for securing our homeland should always be under construction, because the nature of the threat is always changing and evolving.

That leads me to my final question: How do agencies respond to these evolving threats?

A security measure that may work for one facility may not work for another. For example, not every facility might be able to be built 50 feet or more from the nearest public road in order to protect against a vehicle-borne threat.

I also want to know if federal agencies are sufficiently sharing best practices. Is the Department of Defense working with civilian agencies to share its expertise and experience?

For both military and civilian facilities, senior officials at a facility are responsible for determining which security measures should be implemented. However, civilian officials sitting on a local Facility Security Committee may have little or no training in security matters, whereas the commanding officer for a military installation has years of experience and education in security issues.

Most importantly, I want to know what actions different organizations have undertaken since the Navy Yard shooting to improve security at federal facilities.

Many departments and agencies bear some responsibility for securing federal facilities. This includes the Department of Defense and the General Services Administration, and even the Department of Energy. It also includes the Federal Protective Service, a component of the Department of Homeland Security responsible for protecting federal facilities owned or leased by the General Services Administration.

There is no doubt the Federal Protective Service has a difficult mission. That agency employs only about 1,000 law enforcement officers to protect more than 9,000 civilian federal facilities. These facilities are spread out all across the country.

Yet while the Federal Protective Service is responsible for assessing security at each of these facilities, it lacks complete authority to implement security measures. It may recommend installing metal detectors and x-ray screening equipment at a facility, but it is the local Facility Security Committee that decides whether to authorize and pay for those security measures.

As repeated Government Accountability Office (GAO) reports have highlighted, a number of internal management challenges have impeded the Federal Protective Service's ability to protect facilities. For example, the Federal Protective Service must complete the facility security assessments in a timely manner so that it can share them with the offices it protects. Because the Federal Protective Service has been unable to do that, other agencies have sought to complete their own facility security assessments, creating unnecessary duplication and waste.

The Federal Protective Service must also do a better job of tracking and overseeing training for the 14,000 contract guards its uses to protect facilities. The agency must ensure both its federal law enforcement officers and the armed contract security guards it uses are appropriately trained, equipped, and prepared.

Ensuring the training, equipment, and preparedness of federal law enforcement officers and armed contract security guards is central to providing for the security of the facilities safeguarded by the Federal Protective Service. This will require, at minimum, a greater focus on active shooter scenario training. In the wake of the shootings at the Navy Yard and the Wheeling, West Virginia Courthouse, we cannot afford to be ill-prepared for this type of threat.

While Director Eric Patterson has worked hard to improve the Federal Protective Service's performance, the agency has not always received the support it needed from Congress. I want to assure Director Patterson that I am committed to working with him to make the agency more efficient and more effective. We can start by focusing on the cost-saving or cost-neutral solutions that are much more likely to receive broad bipartisan support from Congress.

I hope that today's hearing will help us find better ways to improve security at all federal facilities. I believe there is much to be learned from the Navy Yard tragedy to help us prevent similar incidents in the future. With that, I welcome Dr. Coburn, and I look forward to his opening statement.

**Hearing: "The Navy Yard Tragedy:**
**Examining Physical Security at Federal Facilities"**

**Opening Statement of Dr. Tom A. Coburn, Ranking Member**

Thank you Chairman Carper for continuing this series of important hearings in wake of the Washington Navy Yard shooting, today our focus is on Physical Security at Federal Facilities. Good morning to you witnesses and thank you for being here today. Assistant Secretary Durkovich and Director Patterson, it is very good to have you here and I look forward to hearing your perspective on the security of our Federal Facilities. Director Lewis, welcome back to our committee. Your testimony at our first Navy Yard hearing was appreciated and I look forward to hearing about how your agency has responded since you were last here.

We have to remember the families, co-workers and friends of the innocent men and women were lost during the Navy Yard shooting and the many tragedies before it. What happened here, back in September was a tragedy and we must learn from it. It highlights the need to be ever-vigilant in ensuring that we have effective policies and procedures in place, to ensure individuals at federal facilities are indeed safe. The first hearing in this series exposed several shortcomings in the existing security clearance process and how government agencies and Congress can work together to be more effective. I anticipate this will be the case today, and by working together we have the ability to enhance the security of all of our Federal facilities.

On April 19, 1995, we learned just how vulnerable our federal facilities are when the Murrah Building in Oklahoma City when a truck bomb killed 168 innocent people and injured more than 600. That terrible attack was the catalyst for the federal government to begin looking more closely at the need to secure our federal facilities. Following the 1995 bombing, the Clinton administration established the Interagency Security Committee with a mission of enhancing the quality and effectiveness of physical security at non-military federal facilities. In 2003, this responsibility was transferred to the Department of Homeland Security. And DHS's component, the Federal Protective Service (FPS), took the lead for the protection and security of federally-owned and leased facilities.

After 10 years, it is clear that FPS is not achieving its mission effectively—and our federal facilities in danger as a result. The Government Accountability Office has identified numerous problems in FPS. According to 2010 and 2013 GAO reports, FPS has struggled to ensure that its contracted security officers have necessary training and certifications. For example, GAO found that one contact security company that FPS uses reported that 38 percent of its guards never received their initial X-ray and magnetometer training from FPS, and some of these contracted security officers were working at screening posts. In September, GAO reported that FPS is not providing all of its officers with training for active shooter incidents. That is to say, FPS's contracted security officers are not prepared for the worst-case-scenario events like the Navy Yard tragedy that we are focusing on today. In all, GAO has made 26 recommendations for FPS

since 2010, and only four have been acted on (not yet implemented). I look forward to hearing from GAO today and from the agency about how we can get these recommendations implemented.

The most alarming example of the FPS' problems comes from the DHS inspector general's office. In August 2012, the DHS OIG issued a report on an incident that occurred at the Patrick V. McNamara Federal Building in Detroit, Michigan. FPS' contracted security officers found a bag outside of the federal building and brought it inside. The bag contained an Improvised Explosive Device (IED). The contracted security officers put the bag through the X-ray machine—which they apparently didn't know how to use—and also examined the bag's contents. And they could not discover the IED. It was only identified after the bag was stored under a security console for 21 days. Thankfully, during those three weeks, the IED did not go off. And it is unclear this incident was a malicious attack that failed or a test to show the problem. Either way, it is alarming. If this kind of incident can happen, can we really be 100 percent confident that our federal buildings are safe when FPS is in charge of securing them?

We recognize that securing federal buildings is a responsibility that is spread across the federal government. The responsibility for the security of federal facilities is shared by numerous agencies, they include: CIA, DOD, FPS, State Department, Security Protective Service and uniformed law enforcement officers. We know that our DoD facilities are under the threat of attack—from the Navy Yard Incident to the Fort Hood attack in 2009—as are our embassies and State Department facilities overseas. We should be working together, using the same security standards, accessing the same training and using similar mechanisms for oversight. For example, I have a question about our current policies for combating an active shooter in a Federal facility:

1. Is it consistent among all Federal Agencies?
2. Are we using the "Best Practices" from the private sector?
3. Are these Federal Agencies, who use some of the same contracted security companies, sharing information with each other?

I will focus my attention on DHS and the Federal Protective Service, because that is a focus of our Committee's jurisdiction and we need to hold the Department accountable. This year, our Committee has held hearings looking at key areas of the DHS mission and it seems that wherever we look in DHS we identify big problems and challenges that the Department needs to fix. We know that the overwhelming majority of DHS's employees are dedicated public servants, trying to do a good job. Many of them are putting their lives on the line each day to keep us safe. So we don't say this to unfairly criticize them. While we have seen some areas of improvement in DHS, all-too-often we see that DHS is failing to accomplish many of its core missions.

For DHS to be a successful department, it needs to effectively carry-out its core responsibilities, like protecting non-military federal facilities through the FPS. After a decade, the Department continues to struggle to excel in areas where it has a clear responsibility. We have spent some of

the past year discussing new responsibilities that the Department and Administration want to give to DHS. For example, we know they want more responsibility for cyber security including becoming the lead on cyber security for FISMA for the whole federal government. However, we continue to see including from a recent DHS OIG report that the Department struggles with its own cyber security and information security practices. We know that the administration is working to give DHS more responsibility for cyber security and critical infrastructure, but we continue to see DHS struggle with other missions to oversee and protect critical infrastructure. For example, despite spending a half a billion on the CFATS program since 2007, DHS has not succeeded in making our nation's chemical facilities measurably more secure. The best way that DHS can earn the American people's confidence is by succeeding with the responsibilities that they have already been given, like securing federal facilities.

I know that it's the Secretary's first day on the job today, but if Secretary Johnson is following this hearing today, I hope he will recognize the need to fix programs like the Federal Protective Service. I was proud to support his nomination and think he will be a great Secretary. I know that there is a lot of work on his plate, but I really hope that he is following this hearing today and that he will make strengthening the Federal Protective Service a priority for his tenure. The American people and our federal workforce are counting on DHS and the FPS to make us safe.

Again, I'd like to thank our witnesses for being here today and look forward to this important discussion.

**Statement for the Record**

**Caitlin Durkovich**
**Assistant Secretary for Infrastructure Protection**
**National Protection and Programs Directorate**

**Before the**
**United States Senate**
**Committee on Homeland Security and Governmental Affairs**
**Washington, DC**

**December 17, 2013**

Thank you Chairman Carper, Ranking Member Coburn, and the distinguished members of the Committee. I am pleased to appear before the Committee today to discuss the efforts by the Interagency Security Committee to increase security and resilience at our Nation's Federal facilities.

**Ensuring the Security and Resilience of Critical Infrastructure**

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 that infrastructure. This includes programs to support critical infrastructure owners and operators in enhancing their facilities' security and resilience and coordinating critical infrastructure sectors. These efforts not only prepare our partners for day-to-day activity, but also for large-scale and complex incidents. The National Protection and Programs Directorate (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.

IP is also 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. This plan 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].

[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.

IP conducts onsite 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 identifying methods for how they can improve. Since December 2012, we have 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 addition to serving owners and operators and government officials directly, I serve as Chair of the Interagency Security Committee (ISC) and oversee the development of standards, reports, guidelines, and best practices for civilian Federal facilities through the 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 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 nationwide[2]. The ISC is truly an interagency body exhibiting collaboration and communication among 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. Leadership of the ISC is provided by the Assistant Secretary for Infrastructure Protection, an Executive Director, as well as eight standing subcommittees: Steering, Standards, Technology, Convergence, Training, Countermeasures, Design-Basis Threat, and the Chair Roundtable.

***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, land parcels, and more than 2.5 million tenant employees, and millions of visitors each day from harm. The documents developed by the ISC

[2] The Federal Real Property Council's FY 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.

affect all civilian Federal facilities—regardless of whether they are 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 nonmilitary Federal facilities. The Standard also provides guidance for customization of the countermeasures for Federal facilities and encompasses the following documents:

| | | |
|---|---|---|
| 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 guideline 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 document recommends a set of baseline 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 document provides mail center managers, supervisors, and security personnel with a framework for mitigating risks posed by mail and packages.

The scope and focus of these new initiatives may change as the ISC continues its work. 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 nonmilitary Federal facilities can use as a reference to enhance preparedness for an active shooter incident.

- ***Facility Security Planning:*** 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 cyber security policy and practices.

*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 ongoing 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. Working with partners in the private sector, DHS developed training and other awareness materials to assist owners and operators of critical infrastructure to better train their staff and coordinate with local law enforcement. We have hosted workshops and developed an online training tool targeted at preparing those that work in Federal facilities. These efforts and resources have been well-received and are applicable to Federal facilities as well as commercial spaces and other government buildings.

To date, over 9,700 individuals have viewed DHS's active shooter webinar, over 7,900attendees have participated in over 100 active shooter workshops and exercises nationwide, and over 290,000 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 300,000 times.

Cognizant of this threat and need for resources, the ISC formed a Federal Active Shooter Working Group this past spring. While a number of Federal guidance documents[4] previously existed on active shooter preparedness and response, this Working Group was formed to streamline the existing ISC policy into a single cohesive document. To date, the Working Group has met five times and has reviewed numerous publications and guidance documents including training and materials developed by the Department for commercial facilities. It will also leverage lessons learned from real-world incidents, such as 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.

**Commitment to Securing Federal Facilities**

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 in Kenya, but there are also threats from weather-related events such as Hurricane Sandy, as well as threats to our cyber infrastructure that may have a direct impact on the security of our Federal buildings. While it's 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.

The shooting at the Navy Yard on September 16 served as 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. Ensuring our Federal facilities are secure and resilient is a large undertaking, but the work of our member departments and agencies ensure those responsible for Federal facility security have the tools and resources necessary to mitigate threats.

In closing, I'd 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.

[4] The Design-Basis Threat Report; the Violence in the Federal Workplace: A Guide for Prevention and Response; and Occupant Emergency Programs: An Interagency Security Committee Guide.

**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

**Statement for the Record**

**Leonard E. Patterson**
**Director**
**Federal Protective Service**
**National Protection and Programs Directorate**
**Department of Homeland Security**

**Before the**
**United States Senate**
**Homeland Security and Government Affairs Committee**
**Washington, DC**

**December 17, 2013**

Thank you Chairman Carper, Ranking Member Coburn, and the distinguished members of the Committee. I am honored to testify before the Committee today regarding the mission and operations of the National Protection and Programs Directorate's Federal Protective Service (FPS).

**Mission**

FPS is charged with protecting and delivering integrated law enforcement and security services to over 9,000 facilities owned or leased by the General Services Administration (GSA) and safeguard their more than 1.4 million daily occupants and visitors.

**FPS Authorities**

In performing this mission, FPS relies on the law enforcement and security authorities found in statute[1], agreements with state, local and tribal law enforcement agencies for purposes of protecting Federal property, enforcement of Federal regulations pertinent to conduct on Federal property[2], and our responsibility as a recognized "first responder" for all crimes and suspicious activity occurring at GSA owned or leased property.

**FPS and the Interagency Security Committee**

FPS is an active participant in the work of the Interagency Security Committee (ISC)[3], helping shape standards, guidance and best practices that enable FPS employees to perform their

[1] 40 U.S.C. § 1315
[2] 41 C.F.R., Part 102-74 Subpart C
[3] 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. Following the attack, Executive Order 12977 created the ISC to address "continuing government-wide security" for Federal facilities in the United States. 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

protection mission with consistency, effectiveness, and efficiency. FPS actively participates 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 and the Countermeasures subcommittee. FPS participates in both the Active Shooter-Prevention and Response and the Presidential Policy Directive (PPD) 21 and Compliance working groups that are currently underway. 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 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.

**FPS Law Enforcement Personnel**

FPS directly employs over 1,000 law enforcement officers, inspectors, and special agents who are trained physical security experts and sworn Federal law enforcement officers. FPS 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 to crimes, threats, and other law enforcement activities in support of our protection mission. Law enforcement personnel also oversee guard posts staffed by FPS-contracted Protective Service Officers (PSO), conduct covert security tests, and actively patrol to deter criminal and terrorist activities. Finally, our law enforcement personnel conduct 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.

***Training***

FPS law enforcement personnel receive extensive and rigorous training at the Federal Law Enforcement Training Center (FLETC) in Georgia and in the field. FPS inspectors and special agents complete the FLETC Uniformed Police Training Program or the Criminal Investigation Training Program, respectively. These training programs cover subject areas including, but not limited to, constitutional and Federal criminal law, arrest techniques, defensive tactics, firearms, and active shooter response. Our inspectors also complete FPS-specific law enforcement training, FPS physical security training, and 12 weeks of training in the field under the supervision of a senior, seasoned Inspector. Our special agents complete the specialized FPS Criminal Investigations Special Agent Training Program after the FLETC basic program. In total, FPS inspectors complete approximately 36 weeks of law enforcement and specialized facility security training and our criminal investigators complete a minimum of 17 weeks of law enforcement and criminal investigations training.

---

the Assistant Secretary for Infrastructure Protection, an Executive Director, as well as eight standing subcommittees: Steering, Standards, Technology, Convergence, Training, Countermeasures, Design-Basis Threat, and the Chair Roundtable.

This extensive and rigorous training ensures that FPS law enforcement personnel are able to effectively conduct Facility Security Assessments (FSA) and respond to tens of thousands of calls for service received annually by the FPS, which may entail responding to criminal activity in progress, protecting life and property, and responding to national security events or supporting other law enforcement responding to a critical situation.

***FPS Law Enforcement Authorities***

FPS Law Enforcement Personnel derive their law enforcement authority and powers from section 1706 of the Homeland Security Act of 2002, codified in 40 U.S.C. § 1315. Pursuant to this authority, the Secretary of Homeland Security can designate law enforcement personnel for the purposes of protecting property owned or occupied by the Federal Government and persons on that property.

These designated law enforcement personnel have specific police powers, to include enforcing Federal laws and regulations, carrying firearms, and serving warrants and subpoenas issued under the authority of the United States. Further, they may conduct investigations of offenses that may have been committed against property owned or occupied by the Federal Government or persons on the property. Finally, these law enforcement personnel may make arrests without a warrant for any offense against the United States committed in the presence of the officer or agent or for any felony cognizable under the laws of the United States if the officer or agent has reasonable grounds to believe that the person to be arrested has committed or is committing a felony.

On February 18, 2005, the U.S. Attorney General approved these police authorities in in its *Guidelines For The Exercise Of Law Enforcement Authorities By Officers And Agents Of the Department Of Homeland Security* as required in 40 U.S.C. § 1315. Additionally, pursuant to 41 C.F.R. § 102-85.35, FPS Law Enforcement Personnel provide general law enforcement services on GSA property, and per 41 C.F.R. § 102-74.15, all occupants of facilities under the control of Federal agencies must promptly report all crimes and suspicious activities to FPS.

**Facility Security Assessments (FSAs)**

One of the most important responsibilities of FPS inspectors protecting Federal facilities and those who work or visit these facilities is conducting FSAs at FPS-protected facilities nationwide. FSAs are extensive assessments that document security-related risks to a facility and provide a record of countermeasure recommendations. The process analyzes potential threats toward a facility through a variety of research sources and information and analysis. Upon identification of the threats, the process identifies and analyzes vulnerabilities to a particular facility utilizing Protective Measure Indices.

Assessors utilize the Modified Infrastructure Survey Tool (MIST) to document the existing protective posture at a facility and compare how a facility is, or is not, meeting the baseline level of protection for its Facility Security Level (FSL) as set forth in the ISC's Physical Security Criteria for Federal Facilities standards 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. FPS is working with the DHS Science and Technology Directorate (S&T) to continually review risk assessment methodologies and leverage additional tools as appropriate to improve assessments and recommendations.

**Countermeasures**

Throughout the FSA process, FPS works with stakeholders to identify and gather all necessary information for characterizing the risks unique to each facility. FPS then works in partnership with tenant Facility Security Committees to build a consensus regarding the type of countermeasures appropriate for each individual facility. The decision regarding the optimal combination of physical countermeasures, such as security barriers, X-Ray machines, closed circuit television, and number and type of guard posts staffed by FPS-contracted PSOs is based on a variety of factors including the facility's FSA report, FSL, and the security needs of individual tenants.

**Protective Security Officers**

***Duties***

Approximately 13,000 FPS-contracted PSOs staff guard posts at FPS-protected Federal facilities. 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. FPS PSOs stopped approximately 700,000 prohibited items from entering Federal facilities in 2013.

***Training***

FPS partners with private sector guard companies to ensure that PSOs are prepared to perform their duties. FPS works with the guard companies to ensure the guards have met the certification, training, and qualification requirements specified in the contracts in 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 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 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.

***FPS PSO Authorities***

All PSOs must undergo background investigation checks to determine their fitness to begin work on behalf of the government and are rigorously trained. However, PSOs are not sworn Law Enforcement Officers.

PSOs are employees of private security companies or 'vendors' which are independent contractors doing business with the Federal Government. The relationship between FPS and private-sector vendors is contractual in nature and FPS does not have the authority to deputize PSOs in a law enforcement capability.

FPS contracts with private-sector vendors require that the individual vendor obtain all required state and local licensing, permits, and authorities required for PSOs to carry a firearm and to perform protective services under our contracts. Therefore an individual PSO's authorities to perform protective services are based on state-specific laws where the PSO is employed.

In most instances, PSOs rely on the 'private person' laws, also known as 'citizen's arrest' laws, of a given state as well as that state's laws relating to self-defense, defense of others, and use of force to defend property.

***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 to validate that PSO certifications and training records reflect compliance with contract requirements. In Fiscal Year (FY) 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 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.

**Research and Development**

FPS, in close collaboration with the General Services Administration and S&T, signed a joint Research and Development strategy on July 1, 2013 that identifies key FPS priority areas for research and development:

- Security Operations and Countermeasures: Improve the ability to protect critical infrastructure and ensure continuity of operations while improving the identification, selection, and operational implementation of appropriate countermeasures to effectively and efficiently mitigate hazards to infrastructure and personnel.
- Intelligence and Analysis: Improve the capability to collect timely and accurate intelligence and conduct strategic and operational analysis on incidents, threats, and emerging risks.
- Enterprise-Wide Information/Knowledge Sharing: Improve the interoperability and cooperation of Federal and commercial facilities within the FPS-GSA Critical Infrastructure Enterprise to foster the efficient exchange of information between all levels of government and owners/operators/tenants of critical infrastructure and to coordinate effective responses to, and recovery from, undesirable events.
- Training: Improve the capability to conduct measurably effective, efficient, and repeatable training through the identification and implementation of best practices.

Of note, key elements of this research and development document were briefed to industry via webinar and will be used to inform future investments to ensure that FPS retains the operational capabilities necessary to execute its mission.

**Government Accountability Office Engagement**

While the Government Accountability Office (GAO) has raised some concerns regarding FPS operations in the past, I would like to take this opportunity to discuss the progress FPS has made towards closing-out GAO recommendations.

In FY 2013 alone, FPS has submitted documentation to the GAO for closure and consideration pertaining to 13 GAO recommendations including FPS strategies to enhance its human capital planning and improve tenant communication. Of those presented, six were successfully closed as implemented and seven are pending GAO's internal review for closure.

Specifically, I am pleased to report that significant progress has been made toward closing GAO recommendations regarding FPS's handling of PSO training and oversight. While challenges undoubtedly remain, FPS has successfully closed six outstanding recommendations directly related to this program area and is pending GAO's internal review process for closure consideration for two more.

Additionally, we have made advances towards addressing recommendations relative to our risk-assessment methodology. Specifically, FPS designed its FSA process to meet the requirements of the ISC's Risk Management Process for Federal Facilities and, to ensure that stakeholders have an understanding of the threats they face, has begun to provide a Threat Assessment Report

as part of each FSA. Going forward, FPS will continue to work with the ISC to explore consequences and impacts in the context of Federal facilities security assessments and explore the inclusion of consequences into the FSA process.

Finally, I would like to take this opportunity to thank the GAO for the important service they provide to FPS, its stakeholders, and the American people. FPS understands that GAO audits are conducted to improve performance and accountability within the Federal Government and their contributions are invaluable. As such, FPS remains committed to being transparent and proactive in our effort to provide GAO and Congress with regular updates on the steps we have taken to further enhance, integrate, and transform FPS as we move forward in FY 2014.

**Commitment to Securing Federal Facilities**

In closing, I would like to acknowledge and thank the distinguished members of this committee for the opportunity to testify today. The Federal Protective Service remains committed to its mission of providing safety, security, and a sense of well-being to thousands of Federal employees who work and conduct business in our facilities daily.

I would be pleased to answer any questions you may have.

Statement of

Mr. Stephen F. Lewis
Deputy Director for Personnel, Industrial and Physical Security Policy
Directorate of Security Policy & Oversight
Office of the Under Secretary of Defense for Intelligence

before the
Homeland Security and Governmental Affairs Committee
United States Senate
on

Tuesday, December 17, 2013

Good Morning,

Thank you, Chairman Carper, Ranking Member Coburn and distinguished Members of the Committee –I appreciate the opportunity to appear before you today to address the practices and procedures in the Department of Defense (DoD) regarding facility security. I am Steve Lewis, Deputy Director of the Security Policy and Oversight Directorate in the Office of the Under Secretary of Defense for Intelligence, and I am here today on behalf of Under Secretary of Defense for Intelligence (USD(I)), Michael Vickers.

The USD(I) is the Principal Staff Assistant to the Secretary and Deputy Secretary of Defense for security matters and is responsible for setting overall DoD physical security policy. In this role, the USD(I) provides security policy standards for the protection of DoD personnel, installations, facilities, operations and related assets.

Within the Department, the USD(I)'s security responsibilities are complemented by those of the Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs (ASD (HD & ASA)), who is responsible for the DoD Antiterrorism (AT) Program. The DoD AT Program is an element of the Department's defensive measures used to reduce the vulnerability of individuals and property to terrorist acts, including rapid containment by local military and civilian forces.

In the wake of the recent Washington Navy Yard shooting incident, the Secretary of Defense initiated concurrent independent and internal reviews to identify and recommend actions that addresses gaps or deficiencies in DoD programs, policies, and procedures regarding security at DoD installations and the granting and renewing of security clearances for DoD employees and contractor personnel. The Deputy Secretary of Defense will consolidate key recommendations from each of these reviews into a final report to be provided to the Secretary of Defense. If approved, these recommendations will be addressed in an implementation plan, in coordination with the DoD Components and key Federal agency partners as appropriate.

In order to address the Department's facility security policies and practices, I believe it is important to first describe the requirement for military commanders (or civilian equivalents) to conduct a comprehensive evaluation of an installation, facility, or activity to determine its ability to deter, withstand, and /or recover from

the full range of adversarial capabilities based upon a threat assessment, compliance with established protection standards, and risk management. Based upon the results of these evaluations, active and passive measures are designed to safeguard and prevent unauthorized access to personnel, equipment, installations, and information by employing a layered security concept (i.e., security-in-depth).

With regard to security plans, the Department requires the development and maintenance of comprehensive plans to address a broad spectrum of natural and man-made scenarios. These include the development of joint response plans to adverse or terrorist incidents, such as active-shooter incidents, chemical/biological attacks, unauthorized access to facilities, and tests of physical security. Military commanders (or civilian equivalents), using risk-management principles, are required to conduct an annual local vulnerability assessment, and are subject every three years to a Higher-Headquarters Assessment, such as the Joint Staff Integrated Vulnerability Assessment (JSIVA). A JSIVA is a "vulnerability-based" evaluation of an installation's ability to deter and/or respond to a terrorist incident. Vulnerability-based assessments consider both the current threat and the capabilities that may be employed by both transnational and local terrorist organizations, in terms of their mobility and the types of weapons historically employed.

The Department has worked very hard to foster improvements that produce greater efficiencies and effectiveness in facility security. In its continuing efforts to

harmonize its facility security posture with other Federal departments/agencies, military commanders (or civilian equivalents) located in DoD-occupied leased facility space, including U.S. General Services Administration-owned facilities not on a DoD installation, must utilize the Federal Interagency Security Committee's (ISC) Risk Management process for Federal Buildings. This effort includes the incorporation of the ISC's physical security standards in relevant Department guidance documents (i.e., Unified Facilities Criteria).

We participate in various interagency forums such as the Interagency Security Committee, and Government Facilities and Defense Industrial Base Critical Infrastructure Sector Partnerships, along with representatives from the Department of Homeland Security and other senior-level executives from 53 Federal Agencies/departments. These forums enable the sharing of best practices, physical security standards, and cyber and terrorist threat information in support of our collective resolve to enhance the quality and effectiveness of physical security of Federal facilities.

We have various ongoing initiatives across the Department to enhance facility security, such as the development of an Identity Management Enterprise Services Architecture (IMESA) that will provide an enterprise approach to the sharing of identity and physical access control information, as well as complement ongoing continuous evaluation concept demonstration efforts. The IMESA capability will provide real-time vetting of individuals requiring unescorted access

to DoD facilities against DoD, other Federal, State, and local authoritative data sources. Secure information sharing will enable those facilities with physical access control systems to authenticate individuals' access credentials, authorization, and fitness to enter the facility, vastly enhancing the security of DoD personnel and resources worldwide.

Thank you for your time. I am happy to take your questions.

United States Government Accountability Office

Testimony

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

For Release on Delivery
Expected at 10:30 a.m. EST
December 17, 2013

# HOMELAND SECURITY

# Federal Protective Service Continues to Face Challenges with Contract Guards and Risk Assessments at Federal Facilities

Statement of Mark L. Goldstein, Director
Physical Infrastructure Team

GAO-14-235T

# GAO Highlights

Highlights of GAO-14-094T, testimony before the Committee on Homeland Security and Governmental Affairs, U.S. Senate

## Why GAO Did This Study

As part of the Department of Homeland Security (DHS), the Federal Protective Service (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 security assessments and has approximately 13,500 contract security guards deployed to federal facilities.

This testimony discusses challenges FPS faces in (1) ensuring contract security guards deployed to federal facilities are properly trained and certified and (2) conducting risk assessments at federal facilities. It is based on GAO work issued from 2008 through 2013 on FPS's contract guard and risk assessment programs, and preliminary results of GAO's ongoing work to determine the extent to which FPS and select federal agencies' facility risk assessment methodologies align with federal risk assessment standards. To perform this work, GAO reviewed FPS's and eight federal agencies' risk assessment documentation and compared it to the Interagency Security Committee (ISC) standards. These agencies were selected based on their missions and types of facilities.

## What GAO Recommends

DHS and FPS agreed with the recommendations in GAO's 2012 and 2013 reports to improve FPS's contract guard and risk assessment processes.

View GAO-14-094T. For more information, contact Mark Goldstein, (202) 512-2834 or goldsteinm@gao.gov.

December 2013

# HOMELAND SECURITY

## Federal Protective Service Continues to Face Challenges with Contract Guards and Risk Assessments at Federal Facilities

### What GAO Found

FPS faces challenges ensuring that contract guards have been properly trained and certified before being deployed to federal facilities around the country. In its 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 training on how to respond to incidents at federal facilities involving an active-shooter, FPS has limited assurance that its guards are prepared for this threat. Similarly, an official 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, guards deployed to federal facilities may be using x-ray and magnetometer equipment that they are not qualified to use which raises questions about their ability to screen access control points at federal facilities—one of their primary responsibilities. GAO was unable to determine the extent to which FPS's guards have received active-shooter response and screener training, in part, because FPS lacks a comprehensive and reliable system for guard oversight. 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 2012 recommendation that it develop a comprehensive and reliable system for managing information on guards' training, certifications, and qualifications, it does not yet have such a system.

FPS also continues to face challenges assessing risk at federal facilities. GAO reported in 2012 that FPS is not assessing risks at federal facilities in a manner consistent with federal standards. GAO's preliminary results from its ongoing work on risk assessments at federal facilities indicate that this is still a challenge for FPS and several other federal agencies. Federal standards, such as the *National Infrastructure Protection Plan*'s risk management framework and ISC's risk assessment provisions, state that a risk assessment should include threat, vulnerability, and consequence assessments. Risk assessments help decision-makers identify and evaluate security risks and implement protective measures to mitigate the risk. Instead of conducting risk assessments, FPS is using an interim vulnerability assessment tool, referred to as the Modified Infrastructure Survey Tool (MIST) to assess federal facilities until it develops a longer-term solution. However, MIST does not assess consequence (the level, duration, and nature of potential loss resulting from an undesirable event). Three of the four risk assessment experts GAO spoke with generally agreed that a tool that does not estimate consequences does not allow an agency to fully assess risks. Thus, FPS has limited knowledge of the risks facing about 9,600 federal facilities around the country. FPS officials stated that they did not include consequence information in MIST because it was not part of the original design. GAO will continue to monitor this issue and plans to report its final results early next year.

Chairman Carper, Ranking Member Coburn, and Members of the Committee:

We are pleased to be here to discuss 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), including the challenges associated with FPS's use of contract guards and risk assessments. The 2012 shooting at the Anderson Federal Building in Long Beach, California, the results of our 2009 covert testing, and FPS's ongoing penetration testing demonstrate the continued vulnerability of federal facilities. Although FPS does not protect the Washington Navy Yard, the recent killing of 13 people there once again showed how federal facilities can become targets of violence. 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 to (1) protect the buildings, grounds, and property that are under the control and custody of GSA, as well as the persons on the property; (2) enforce federal laws and regulations aimed at protecting such property and persons on the property; and (3) investigate offenses against these buildings and persons.[2] FPS conducts its mission by providing security services through two types of activities:

- physical security activities—conducting security assessments and recommending countermeasures aimed at preventing incidents—and
- 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

[1]GAO, *High Risk Series: An Update*, GAO-13-283 (Washington, D.C.: 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."

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 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. To address this issue, we made several recommendations which FPS agreed to implement. These recommendations and their status are discussed later in this statement.

This testimony discusses challenges FPS faces in (1) ensuring contract security guards deployed to federal facilities are properly trained and certified and (2) conducting risk assessments at federal facilities. It is based on our reports and testimonies issued from 2008 through 2013 on

[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.

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

FPS's contract guard and risk assessment programs.[6] A list of these related products appears at the end of my statement. As part of the work for these products, we reviewed relevant statutes and federal guidance; examined FPS contract guard and risk assessment processes and procedures; reviewed a sample of contract guard files; conducted site visits to FPS's 11 regions where we interviewed FPS officials; and interviewed FPS's 31 guard companies and 4 risk management experts. This testimony is also based on preliminary results of our ongoing effort to determine the extent to which FPS and select other federal agencies assess risk in accordance with federal risk assessment standards. We plan to issue our report early next year. As part of that work, we reviewed and analyzed risk assessment documentation and interviewed officials at nine federal agencies and compared each agency's methodology to Interagency Security Committee (ISC) 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 ongoing work from August 2012 to December 2013 in accordance with generally accepted government auditing standards. Also, our previously issued testimonies and reports were conducted 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.

[6]GAO, *Federal Protective Service: Challenges with Oversight of Contract Guard Program Still Exist, and Additional Management Controls Are Needed*, GAO-13-694 (Washington, D.C.: September 2013); GAO, *Federal Protective Service: Actions Needed to Assess Risk and Better Manage Contract Guards at Federal Facilities*, GAO-12-739 (Washington, D.C.: 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, D.C.: 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, D.C.: June 2008).

Additional details about the scope and methodology can be found in each of these related reports.

## 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,[7] FPS faces challenges providing active-shooter response training to all of its guards. 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. 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.[8] 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.

[7]GAO-13-694.

[8]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.

We were unable to determine the extent to which FPS's guards have received active-shooter response training, in part, because FPS lacks a comprehensive and reliable system for guard oversight (as discussed below). When we asked officials from 16 of the 31 contract guard companies we contacted if their guards had received training on how to respond during active-shooter incidents, responses varied.[9] For example, of the 16 contract guard companies we interviewed about this topic:

- officials from eight contract guard companies stated that their guards had received active-shooter scenario training during FPS orientation;
- officials from five guard companies stated that FPS has not provided active-shooter scenario training to their guards during the FPS-provided orientation training; and
- officials from three 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.

DHS and FPS agreed with our 2013 recommendation to 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.

## Some FPS Contract Guards Have Not Received Required Screener Training

As part of their 120 hours of training required by FPS, 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,[10] 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.[11] In response to those reports, FPS

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

[10]GAO-13-694.

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

stated that it planned to implement a program to train its inspectors to provide screener training to all its contract guards.

We were unable to determine the extent to which FPS's guards have received screener training, but information from guard companies we contacted indicate that 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.

As noted above, FPS agreed with our 2013 recommendation to determine which guards have not had screener training and agreed to provide it to them.

## FPS Lacks Effective Management Controls to Ensure Contract 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 2012 recommendation to develop a comprehensive and reliable system for contract guard oversight, it has not yet established 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 reported 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.[12] 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 |
| 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** | **117**[a] |

Source: GAO analysis of contract guard company data reported in 2013.

Note: These results are nongeneralizeable and based on a review of 276 randomly selected guard files for 11 of 117 FPS guard contracts.

[a]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 review guard companies' guard files monthly.

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

From March 2012 through March 2013, FPS reviewed more than 23,000 guard files.[13] 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, that documented 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.[14] As a result of the lack of management controls, FPS is not able to provide reasonable assurance that guards have met training and certification requirements.

DHS and FPS agreed with our 2013 recommendation to develop and implement procedures for monthly guard-file reviews to ensure consistency in selecting files and verifying the results.

## FPS Continues to Face Challenges with Assessing Risk at Federal Facilities

We reported in 2012 that FPS is not assessing risks at federal facilities in a manner consistent with federal standards. The preliminary results of our ongoing review of risk assessments of federal facilities indicate that this is still a challenge for FPS and several other federal agencies. Federal standards such as the *National Infrastructure Protection Plan's (NIPP)* risk management framework and ISC risk assessment provisions call for a risk assessment to include threat, vulnerability, and consequence assessments. Risk assessments help decision-makers identify and evaluate security risk and implement protective measures to mitigate risk. Moreover, risk assessments play a critical role in helping agencies tailor protective measures to reflect their facilities' unique circumstances and enable them to allocate security resources effectively.

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

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

Instead of conducting risk assessments, FPS uses an interim vulnerability assessment tool, referred to as the Modified Infrastructure Survey Tool (MIST), with which it assesses federal facilities until it develops a longer-term solution. According to FPS, MIST is allowing it to resume assessing federal facilities' vulnerabilities and recommend countermeasures—something FPS has not done consistently for several years. However, MIST has some limitations. Most notably, it does not assess consequence (the level, duration, and nature of potential loss resulting from an undesirable event). Three of the four risk assessment experts we spoke with generally agreed that a tool that does not estimate consequences does not allow an agency to fully assess risks. FPS officials stated that they did not include consequence information in MIST because it was not part of the original design and thus requires more time to validate. MIST also was not designed to compare risks across federal facilities. Consequently, FPS does not have the ability to take a comprehensive approach to risk management across its portfolio of 9,600 facilities and recommending countermeasures to federal tenant agencies.

As of December 2013, according to an FPS official, FPS had used MIST to complete vulnerability assessments of approximately 1,800 federal facilities and have presented approximately 1,000 of them to the facility security committees. We will continue to monitor this issue and plan to report the results early next year.

DHS agreed with our 2012 recommendations to incorporate NIPP's risk management framework in any future risk assessment tool; coordinate with federal agencies to reduce any unnecessary duplication in FPS's assessments; and address limitations with its interim tool to better assess risk at federal facilities. However, it has not yet implemented them.

## Contact Information

For further information on this testimony, please contact Mark Goldstein at (202) 512-2834 or by email at GoldsteinM@gao.gov. Individuals making key contributions to this testimony include Tammy Conquest, Assistant Director; Geoff Hamilton; Bob Homan; and Sara Ann Moessbauer.

**Testimony of Stephen Amitay, Esq.**
**Executive Director and General Counsel**

**National Association of Security Companies (NASCO)**

**Before the**
**Senate Homeland Security and Government Affairs Committee**

**Hearing on**
***"The Navy Yard Tragedy: Examining Physical Security for Federal Facilities"***

**December 17, 2013**

Testimony of Stephen Amitay, Esq.
Executive Director and General Counsel
National Association of Security Companies (NASCO)
Before the
Senate Homeland Security and Government Affairs Committee
Hearing on
"The Navy Yard Tragedy: Examining Physical Security for Federal Facilities"
December 17, 2013

Introduction

The Washington Navy Yard attack raised important issues and challenges related to federal facility security, access control, and personnel background screening. Unfortunately, the Navy Yard attack followed several other shootings at federally protected facilities over the past five years.[1] With such "active shooter" incidents on the rise, federal agencies responsible for federal facility security and their contract security partners who provide security personnel for those facilities must work together to address current federal facility security issues and develop new efficient and effective strategies to reduce the risks of such incidents as well as other threats.

Federal executive branch agencies are responsible for protecting over 370,000 non-military buildings and structures.[2] The Department of Homeland Security's (DHS) Federal Protective Service (FPS) is the primary agency responsible for providing law enforcement and related security services for the approximately 9,600 federal facilities under the control and custody of the General Services Administration (GSA). FPS has about 1,200 full-time employees and about 13,500 contract "Protective Security Officers" (PSO's) deployed at thousands of federal facilities (generally Federal Security Level III and IV facilities) of GSA's 9,600 facilities.[3] The remainder of the federal buildings and structures are protected by some three dozen other federal executive branch agencies. Not including the military services, there are approximately 35,000 private security officers working for various federal agencies.[4]

---

[1] 2009 Holocaust Museum, 2009 Fort Hood, 2010 Pentagon, 2010 Las Vegas Courthouse, 2012 Long Beach Federal Building, 2012 Birmingham Courthouse, 2013 Wheeling (WV) Federal Building.

[2] GAO:FACILITY SECURITY: Greater Outreach by DHS on Standards and Management Practices Could Benefit Federal Agencies GAO-13-222, Jan 24, 2013 Page http://www.gao.gov/assets/660/651529.pdf

[3] GAO: FEDERAL PROTECTIVE SERVICE: Challenges with Oversight of Contract Guard Program Still Exist, and Additional Management Controls Are Needed GAO-13-694, Sep 17, 2013 http://www.gao.gov/assets/660/657920.pdf This report claims "FPS has about 1,200 full-time employees and about 13,500 contract security guards deployed at approximately 5,650 (generally level III and IV facilities) of GSA's 9,600 facilities." As to which facilities actually have PSO's onsite, a 2011 GAO Report stated that "FPS provides security personnel to about 2,360 (GSA) facilities..." GAO: FEDERAL FACILITY SECURITY: Staffing Approaches Used by Selected Agencies GAO-11-601 June 2011. http://www.gao.gov/assets/330/320625.pdf

[4] The largest amount of contract security officers work for FPS (approx. 13,S00), the United States Marshal Service (approx. 5,000), and the Department of Energy (approx. 5,000). Other federal agencies/instrumentalities that use contact security include: IRS, NASA, FAA, USDA, DOT, DOC, HHS, SSA, NARA, DOL, FDIC, US Coast Guard, State, DIA,

NASCO is the nation's largest contract security trade association, whose member companies employ more than 300,000 security officers across the nation servicing commercial and governmental clients. NASCO member companies and companies in affiliated NASCO "Government Security Contractors Caucus" provide security officers to numerous federal agencies for the protection of federal facilities including the majority of FPS PSO's. Since 2007, NASCO has been working with FPS, as well as Congress and the GAO, to address issues related to the "Protective Service Officer Program (PSOP)" (formerly known as the "Contract Guard Program"). Many of the issues and challenges identified with the PSOP have been laid out in various GAO Reports.

To further ensure the protection of federal facilities and their occupants and visitors, FPS and its security contractors need to continue to work together to make improvements related to training, oversight, recordkeeping, PSO instructions and post orders, and there also needs to be improvement in the lines of communication between FPS headquarters, the regional officials, contract officers, federal tenants, and contractors. FPS is well aware of these issues and there is no doubt that there has been substantial progress being made to address them.

Since the appointment of Director Patterson in 2010, who in turn brought on an Assistant Director for Training, the degree of dialogue and breadth cooperation between FPS and security contractors has been unparalleled. While things might not be moving as fast as GAO and security contractors would like, FPS' commitment to improving the PSO Program at FPS is unquestionable and this commitment is evidenced by its work, often in close partnership with contractors, on numerous activities and initiatives. Currently, NASCO and FPS are working together on a host of issues related to PSO training that will improve the content and delivery of PSO training, standardize PSO training, as well as increase the capability to validate that training. Better and smarter trained PSO's mean better and smarter security at federal facilities. PSO's. Additionally, in the field there have been improvements, driven from headquarters, which have brought greater standardization in the contract process and the treatment of security contractors and PSO's. Much still needs to be done, and can be done, but FPS's management of its contract security force has come a very long way in the past decade. NASCO looks forward to continuing to work closely with Director Patterson and FPS to improve federal facility security through the cost-effective use of contract security officers.

Overview of FPS Activities to Improve the Protective Security Officer Program (PSOP)

Below are highlight of current activities and improvement being made related to the PSOP

In the critically important area of providing x-ray and magnetometer training for PSO's, a deficiency GAO has highlighted on numerous occasions, FPS, working with NASCO, is about to launch a pilot program that will train and certify security contractor instructors so that they can provide the training instead of requiring that PSO's be trained by stretched thin FPS personnel. As GAO has noted, this current situation has resulted in PSO's never receiving the training. And with FPS increasing the PSO screener training to

---

NRC, Holocaust Museum, and Smithsonian. Private screening companies/personnel are also being utilized successfully at various airports around the United States under the TSA Screening Partnership Program.

16 hours (with an annual 8 hour refresher), the need for its security contractors to be conducting this training is acute.

FPS is also moving to increase "active shooter" training for PSO's. Since the Navy Yard attack, FPS has provided security contractors with new "active shooter instructions" to distribute to PSO's and add to all post orders, and also there will be a new chapter on active shooter in the upcoming revision of the Security Guard Information Manual (SGIM). Nevertheless, it seems clear that actual "active shooter" training is also needed and FPS is also now in the beginning phases of developing such training. We look forward to working with FPS on developing this active shooter training, which is expected to be provided by the security contractors.

While these above FPS training initiatives essentially represent FPS "coming up to speed" with what some other federal agencies that use contract security officers are already doing, these are significant steps in the right direction that will increase training efficiency and effectiveness and lead to better security being provided at federal facilities.

In another training initiative, FPS is working with NASCO and security contractors to revise and standardize the PSO training lesson plans as well working to improve the firearms training and qualifications for PSO's.

FPS also is reaching out to other federal agencies, to see how they are training and managing their contract security officers, and importantly, they are including FPS security contractors in this outreach. Later this month, through an agreement between FPS and DoE, DoE will allow FPS and a group of FPS security contractors attend a DoE "simulated active shooter scenario" that DoE is providing for its contract security officers. The goal is to continue to increase active shooter awareness and response procedures, and share best practices between DoE and FPS on active shooter reaction and response procedures.

FPS is also (finally) coming out with a much needed revision of the "Security Guard Information Manual" (SGIM), the PSO bible. The SGIM governs and instructs PSO's on how to act and not following the SGIM is considered a contract violation. Unfortunately, the degree of contractor input into this revision process was minimal, and certain long-standing issues such as instructions related to a PSO's authority to act (and potentially liability for acting) in extreme situations may not be adequately addressed. However, FPS officials have said that the new version of the SGIM (now called the Security Manual and Resource Tool "SMART" book) will be a version control document that is founded on a quality management process that will allow for incorporating improvements and updates more easily.

FPS is also conducting a comprehensive review of PSO Post Orders and looking to standardize and update them. NASCO commends this effort as many current post orders are fairly nebulous and vague. However, new post orders, in addition to being standardized, need to be facility specific and tailored to the specific post.[5]

[5] For instance, in some facilities there will be a "duress button" that sets off an alarm; however, there is nothing in the post orders about what to do upon setting off the alarm. Post orders should also have information on the closest fire alarm, and other location/post specific information.

In the area of security contractor oversight and the verification of PSO training and certifications (an often raised issue by GAO) in many instances the issue is not that a PSO did not receive one of the 24 required PSO trainings and certifications, but instead it is an issue of poor recordkeeping/file inspections and conflicting interpretations of contract requirements. To address this problem, FPS has revised its Contractor Officer Representative (COR) training and is bringing on board 39 dedicated Contracting Officer Representatives. This new COR cadre will not be spread thin doing other FPS duties as many current FPS inspectors doing COR duties are now. This should result in better FPS oversight of contract compliance, quicker resolution of contract issues, and more efficient data management.

I will return to these PSOP related issues later in my testimony after discussing some of the bigger picture threat and risk mitigation issues related to physical security at federal facilities.

Federal Employee and Contractor Personnel Screening and Access Control

As to the issue of federal employee and contractor security clearance screening that played a prominent role in the Navy Yard attack, this is an area where NASCO and it members are not involved. It is encouraging though that even before the attack, a major government-wide reform effort, initiated by DNI and OPM was underway to revise federal investigative standards so that they will incorporate the concept of "continuous evaluation" which will allow for information such as a recent arrest or conviction anywhere to become available on a timely basis for background screening officials. Also, the Administration's recent "Insider Threat" initiative seeks to complement the continuous evaluation concept by incorporating data from a broad set of data sources to identify problematic behavioral trends. [6] Without a doubt, improvements must be made to the security screening process so that someone like Navy Yard shooter, who after he received his security clearance was arrested several times and was also reported to the Navy as being mentally unstable, will have his access authority revoked.

As to access control at federal facilities, PSO's and other contract security officers at federal facilities are very involved in this process. (Both at the Navy Yard and the Holocaust Museum contract security officers at access control points were killed in those attacks). However, contract security companies, while they do have expertise in setting appropriate access control policies, do not generally have a say in the access control policies at federal facilities. One obvious access control policy solution related to the Navy Yard attack would be to require all federal employees and contractors to be subject to screening at federal facilities or at least implement random screening of employees and contractors.

Federal Facility Security Elements and the Interagency Security Committee

Federal facility security threats include terrorist attacks, active shooters, workplace violence, anti-government protests, unauthorized access, theft, and there is no doubt that protecting federal facilities and their occupants and visitors is an ongoing challenge for federal agencies. Federal facility threat

[6]Testimony of Mr. Greg Marshall, Chief Security Officer, U.S. Department of Homeland Security, before the House CHS Subcommittee on Oversight and Management Efficiency, Hearing: "Facility Protection: Implications of the Navy Yard Shooting on Homeland Security." October 30, 2013.
http://homeland.house.gov/sites/homeland.house.gov/files/documents/Testimony-Marshall.pdf

mitigation involves conducting facility security assessments (FSA's) and setting/re-setting facility security levels, devising and recommending countermeasures to mitigate risks, considering and adopting countermeasures, and then implementing countermeasures. The conduct of federal facility security assessments and the process for the consideration and adoption of security countermeasures are "governed" by Standards promulgated by the Federal Interagency Security Committee (ISC). Created by Executive Order after the Oklahoma City bombing, the ISC's mandate is "to enhance the quality and effectiveness of physical security in, and the protection of buildings and nonmilitary Federal facilities in the United States. The ISC standards apply to all nonmilitary Federal facilities in the United States - whether government-owned, leased or managed; to be constructed or modernized; or to be purchased."[7]

Earlier this year, the ISC came out with the "Risk Management Process: An Interagency Security Committee Standard." The Standard creates one formalized process for defining the criteria and process that should be used in determining the Facility Security Level of a Federal facility, determining risks in Federal facilities, identifying a desired level of protection, identifying when the desired level of protection is not achievable, developing alternatives, and risk acceptance, when necessary. The Standard provides an integrated, single source of physical security countermeasures for all non-military Federal facilities and guidance for countermeasure customization for Federal facilities.[8]

The Standard incorporates and supersedes numerous previous ISC Standards related to federal facility security and not only provides an introduction to the risk management process but also outlines the approach necessary to identify, assess, and prioritize the risks to Federal facilities.

As the Standard notes, consistent with Executive Order 12977, it is "intended to be applied to all buildings and facilities in the United States occupied by Federal employees for nonmilitary activities." [9] In fact, EO 12977 states that "Each executive agency and department shall cooperate and comply with the policies and recommendations of the Committee issued pursuant to this order" and the Order, as amended, gives DHS the responsibility to monitor federal agency compliance with ISC Standards. [10]

However, often throughout the risk management assessment process and in the process of considering and adopting suitable countermeasures, the requirements of the ISC Standards are not met.

Earlier this year, GAO released report titled Report "Greater Outreach by DHS on Standards and Management Practices Could Benefit Federal Agencies."[11] In the Report, GAO noted that ISC Standards "are developed based on the collective knowledge and physical security expertise of ISC member agencies

---

[7] http://www.dhs.gov/interagency-security-committee

[8] "The Risk Management Process: An Interagency Security Committee Standard" August 2013, First Edition. http://www.dhs.gov/sites/default/files/publications/ISC_Risk-Management-Process_Aug_2013.pdf

[9] ISC RM Standard, page iii

[10] Executive Order 12977 of October 19, 1995. Federal Register Vol. 60, No. 205 Tuesday, October 24, 1995 http://www.gpo.gov/fdsys/pkg/FR-1995-10-24/pdf/95-26497.pdf

[11] GAO Facility Security Report January 2013. (See footnote 2).

and, therefore, reflect leading practices in physical security." More so, "the (u)se of ISC standards may be beneficial because they provide agencies with tools and approaches for consistently and cost-effectively establishing a baseline level of protection at all facilities commensurate with identified risks at those facilities. By using the standards to determine the level of protection needed to address the unique risks faced at each facility, agencies may be able to avoid expending resources on countermeasures that are not needed."

It seems very clear that ISC Standards provide effective guidance for all aspects of facility security.

However, in a survey of 32 federal agencies, GAO found that "the extent of agencies' use of ISC standards varied—with some agencies using them in a limited way." In this vein, at a House hearing last month on federal facility security, GAO testified that "our ongoing review of nine 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. (As a result) these agencies may not have a complete understanding of the risks facing...federal facilities.[12]

The GAO Report further found that "agencies' reasons for making limited use of ISC standards reflect a lack of understanding by some agencies regarding how the standards are intended to be used."

The Report acknowledges though that there are other sources for developing physical security programs for federal facilities in addition to ISC Standards, most notably, an agency's institutional knowledge or subject matter expertise in physical security. Agencies also turn to non-governmental experts, including private security companies, to establish their physical security plans.[13] Finally, agencies also are guided by federal statutes and regulations, state or local regulations and agency/facility specific information such as mission and the type, use, and location of their facilities.

Thus, while some agencies may not be putting facility security at risk by limiting their use of ISC Standards; nonetheless, the pervasive non-compliance with ISC Standards by federal agencies responsible for federal facility protection, whether intentional or as a result of a "lack of understanding" the standards, is not a good situation.

In one example of ISC standard non-compliance, an FPS security contractor encountered a situation where upon taking over a contract for the security/access control at a federal building was informed by the tenant agency that in order to maintain a "free and open culture" the agency had a "security" policy of

---

[12] Testimony of Mark Goldstein, Director of Physical Infrastructure Issues, before the House CHS Subcommittee on Oversight and Management Efficiency, Hearing: "Facility Protection: Implications of the Navy Yard Shooting on Homeland Security." October 30, 2013.
http://homeland.house.gov/sites/homeland.house.gov/files/documents/Testimony-Goldstein.pdf

[13] GAO Facility Security Report January 2013. One official told GAO that "his agency contracts with a security company that has extensive knowledge and experience in providing security and law enforcement to high profile institutions across the federal government, and that this knowledge is used in managing the agency's security program." Page 8.

not screening anyone coming into the building --- in clear non-compliance with ISC standards. The security contractor reported this situation to FPS and FPS then persuaded the tenant to implement some screening. Other security contractors too have seen instances of agencies ignoring ISC standards or not being aware of them. As will be discussed later, the central role of federal facility tenants in approving security policies for federal facilities has clearly been identified as a facility security concern.

Unfortunately, due to staff and resource limitations, the ISC does not formally monitor agencies' compliance with ISC standards. The ISC does hold regular meetings and has working groups where information is shared about agency compliance, but, as GAO reports, "this approach does not provide a thorough or systematic assessment of ISC member agencies' use of the standards, and provides no information on non-member agencies' physical security practices." [14]

The GAO recommended that the ISC "conduct outreach to all executive branch agencies to clarify how the standards can be used in concert with agencies' existing physical security programs." Also recommended, "To help agencies make the most effective use of resources available for physical security across their portfolios of facilities, develop and disseminate guidance on management practices for resource allocation as a supplement to ISC's existing physical security standards." ISC has stated in its 2012 to 2017 action plan that it plans to establish protocols and processes for monitoring and testing compliance with its standards by fiscal year 2014.

Greater education on, use of, and compliance with ISC Standards by federal agencies/tenants should lead to more effective and efficient federal facility security. ISC should work to implement the recommendations of GAO and DHS should devote more resources to the ISC for educational and compliance efforts.

Federal Facility Security Assessments

As mentioned above, GAO has found 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, and as a result, "FPS and the other non-compliant 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)." Risk assessments (facility security assessments) are the foundation upon which an effective facility security policy is built and FPS needs to improve its FSA capabilities in both efficacy (and compliance with ISC Standards) as well as being able to do FSA's in a timely fashion. Several years ago FPS attempted to develop a comprehensive risk assessment tool (RAMP) that failed and set FPS back in the FSA arena. The current FPS risk assessment tool (MIST) in addition to not being aligned with ISC standards also has other limitations according to GAO.

In addition, in a recurring theme at FPS, the persons who are responsible for doing FSA's (FPS inspectors) are also doing law enforcement and investigative related work, acting as contracting officer representatives (COR's), providing screener and orientation training to PSO's, conducting PSO firearm qualification and doing other duties. They are spread thin, and this can further hamper the ability of FPS

[14] Ibid. page 12.

to conduct quality FSA's in a timely manner. As FPS is now doing with the creation of a much needed dedicated COR force, it might consider creating a dedicated FSA force, but such a force would need better training, tools and quality control management. As to better tools, FPS should look to the private sector and other agencies to find an effective risk assessment tool instead of trying to develop one. There are commercial off the shelf risk assessment tools available. In addition, FPS could free up Inspectors and increase the amount of FSA's completed by outsourcing FSA's to companies that have experts who specialize in such work and are currently doing FSA's for nuclear facilities, critical infrastructure, and high risk commercial buildings.

Federal Facility Security Committees

A critical player in prioritizing and mitigating threats to federal facilities is the "Facility Security Committee (FSC)." As explained in the ISC Risk Management Process Standard, the FSC consists of representatives of all Federal tenants in the facility, the security organization (Federal Protective Service for General Services Administration (GSA) owned and operated facilities), and the owning or leasing department or Agency. The FSC is responsible for determining the Facility Security Level for the facility, addressing the facility-specific security issues addressed in the facility security assessment and approving the implementation of security countermeasures and practices recommended by the security organization.[15] These are very serious facility security responsibilities.

In GSA owned/leased building, FPS is responsible for doing the FSA and then recommending (and explaining) the appropriate countermeasures to the FSC. However, it is clear that "the decision to implement those recommendations and mitigate the risk or to accept risk as part of a risk management strategy is that of the FSC."[16]

In past GAO Reports, and in contractor dealings with FSC's and tenant agencies, there have been serious issues as to whether FSC's are making "informed risk-based decision regarding the mitigation or the acceptance of risk" as required by the ISC Risk Management Process Standard. In a 2010 GAO Report, GAO noted something that FPS and security contractors have experienced first-hand at federal facilities; "tenant agency representatives to the FSC generally do not have any security knowledge or experience but are expected to make security decisions for their respective agencies." [17]

Security contractors working at federal facilities have observed that often at FSC meetings the lead agency will call the shots and ignore FPS recommendations. Tenant representatives do not want to be there, are disinterested and therefore FSC meetings are also not well attended. In addition, for some FSC's there is a greater interest in providing "customer service" than building security. [18]

While GAO also opined that tenant representatives on the FSC may not be getting adequate information from FPS (and some observers believe that FPS needs to do a "better sales job" with the FSC's);

[15] ISC RM Process Standard.
[16] ISC RM Process Standard. 6.0 "The Risk Informed Decision Making Process"
[17] GAO: HOMELAND SECURITY "Addressing Weaknesses with Facility Security Committees Would Enhance Protection of Federal Facilities" GAO 10-901 August 2010 http://www.gao.gov/new.items/d10901.pdf
[18] At some federal building PSO's are not allowed to "hand check" employee ID's when necessary.

nonetheless, the bottom line is that security decisions for federal facilities are often being made by persons with no education or training in risk mitigations and security. Also, with shrinking agency budgets combined with the fact that "many of the FSC tenant agency representatives do not have the authority to commit their respective organizations to fund security countermeasures"[19] it is becoming increasingly more likely that recommended and necessary security countermeasures are being voted down solely because of cost concerns.

Whether it be for a lack of understanding of the risks or a lack of a funding commitment, both of these scenarios are a prescription for increasing risks at federal facilities. There are though solutions to the above described FSC problems.

Last Congress, this Committee passed a bill (endorsed by NASCO), which introduced by former Chairman Lieberman and former Ranking Member Collins, that addressed both the FSC member lack of training/education issue as well as the refusal of an FSC (for whatever reason) to implement recommended countermeasures issue. In S.772, 'Supporting Employee Competency and Updating Readiness Enhancements for Facilities Act of 2012' (SECURE Act) there was a provision that said that if the DHS Secretary in coordination with the ISC, "determines a Federal facility (protected by FPS) to be in noncompliance with Federal security standards established by the Interagency Security Committee or a final determination regarding countermeasures" and the facility loses an appeal and still does not implement the countermeasure, then "The Secretary may assess security charges to an agency that is the owner or the tenant of (the) Federal facility... for the costs of necessary security countermeasures."[20]

Also in the SECURE Act, there is a provision that requires that "before serving as a member of a Facility Security Committee, an employee shall successfully complete a training course that meets a minimum standard of training as established by the Interagency Security Committee" that is "commensurate with the security level of the facility." [21]

In the new ISC Risk Management Standard, there is too an FSC education requirement. "Federal employees selected to be members of a Federal FSC will be required to successfully complete a training course that meets the minimum standard of training established by the ISC." However, with no way to monitor/enforce compliance it is likely the percentage of current FSC members at federal facilities who have taken required training courses is small.

Congress should work with DHS, who chairs the ISC, FPS and all federal agencies to make sure that FSC members are taking the required training. The safety of the employees and visitors in federal facilities also needs to be funding priority. FPS will need to work harder with it federal clients to identify and

---

[19] Ibid.

[20] S. 772 "Supporting Employee Competency and Updating Readiness Enhancements for 4 Facilities Act of 2012" http://thomas.loc.gov/cgi-bin/query/z?c112:S.772.RS:/ SEC. 247. COMPLIANCE OF FEDERAL FACILITIES WITH FEDERAL SECURITY STANDARDS.

[21] S. 772 SECURE Act of 2012, SEC. 264. FACILITY SECURITY COMMITTEES (c) "Training for Members"

implement the most cost-effective countermeasure appropriate for mitigating vulnerability, but in the end, necessary security should never fall victim to budget cuts.

Effective Countermeasures: The Use of Protective Security Officers

In thousands of GSA facilities a primary security countermeasure is the deployment of contract PSO's through the FPS Protective Security Officer Program (formerly the "Contract Guard Program."). In other facilities, lesser security countermeasures, such as cameras and perimeter lighting, may be deployed to mitigate risk at these facilities.

PSO's are the most visible component of the FPS' operations, and they are the "eyes and ears" of the FPS mission. As part of their assigned duties, PSO's are expected to; control access to specific areas of a facility (access control includes checking visitor and employee identification; operating security equipment such as x-ray machines and Magnetometers to screen for prohibited materials;) enforce property rules and regulations; detect and report criminal acts; stop and if possible, detain persons engaging in criminal activities; provide security against loss from fire or mechanical equipment failure; respond to emergency situations involving the safety and security of the facility; and act occasionally as a crowd monitor to maintain order.[22] PSO's are specifically "authorized to detain people if it is necessary to ensure order and safety at (the) assigned facility."[23]

FPS PSOP Security Related Issues and Initiatives

As mentioned in the introduction, since 2007, NASCO and its members have worked with FPS on issues related to the FPS PSOP. Below are some of the current initiatives and issues which relate to the performance and capabilities of PSO's to provide security at federal facilities.

Active Shooter

On the subject of active shooter response, there are two issues. One is training and the other is authority to act. As to training, as mentioned, while other agencies are already providing active shooter training to its contract security officers, the current FPS "training" is light to non-existent.[24] Active shooter may come up in passing during a 2 hour segment of the 8 hour FPS provided orientation training, and some contractors provide their PSO's with active shooter resources, but FPS needs to do more for the PSO's on active shooter, and the agency is aware of this fact.

FPS recently provided PSO's with "Active Shooter Instructions" that are now part of their post orders and FPS has said that there will be additional PSO instruction on active shooter in the revised Security Guard Information Manual (now the SMART Book). FPS is also developing actual active shooter training for

[22] Federal Protective Service • "Security Guard Information Manual", 2008 Revision Chapter 2.1 "Your Roles and Responsibilities."

[23] FPS SGIM, Chapter 3.6 "Detainment Authority"

[24] DoE, State, Commerce, Holocaust Museum, NASA, Pentagon Force Protection Agency, IMF and World Bank all provide active shooter training for contract security officers. See Sept. 2013 GAO Report (footnote 2).

PSO's which could be incorporated into or added to the contractor provided portion of PSO training. Given the difficulties that FPS has with providing the mandated screener training to PSO's, and FPS' pilot program to have the screener training done by the security contractors, it is unimaginable that FPS would take on the active shooter training responsibility. FPS is reviewing the active shooter training other federal agencies are providing to contract security officers, and FPS is including its security contractors in that review process. NASCO hopes that FPS will also work with security contractors to develop an appropriate and effective active shooter training course for PSO's. This could involve contractor instructors getting trained and certified by FPS/FLETC to provide active shooter training to PSO's (as will happen in the screener training pilot program). Any active shooter training should be building specific, scenario specific, incorporate actual drills on a regular basis after the initial training, and consider if there are armed federal employees in the facility (i.e. DEA, FBI, DHS, ICE or other armed federal agents).

Authority to Act and Arrest Authority

An issue that is often raised in situations in federal facilities where violence, weapons, or the potential for violence is present is the ability/authority of PSO's to act, and the related legal issue of what constitutes "detaining" an individual, and what constitutes "arresting" an individual. PSO's are often put in situations where a person will enter a federal facility and starts acting strange or violent or potentially violent, or the person might have a weapon. In some instances, PSO's have detained individuals (including handcuffing them) and then later been sued for false arrest. Under FPS regulations, all PSO's must be licensed by the state where they are posted a federal facilities. As all PSO's are armed, this would require getting an armed officer license in that state. In some states, such as Virginia, licensed armed officers are given state statutory authority to arrest people that are committing crimes on the property where they work. With such arrest authority, a PSO can more confidently and assuredly detain a violent person at a federal facility and not worry about a false arrest charge. However, under FPS rules for PSO's (contained in the SGIM) it says that "even if you are deputized under current or past employment endeavors, you do not have arrest authority while performing on an FPS contract." [25] A violation of the SGIM is a violation of the contract.

Also as to what constitutes permissible detainment by a PSO is also very vague. The SGIM states that "as an FPS security guard you are authorized to detain people if it is necessary to ensure order and safety at your assigned facility. You should detain a person only when absolutely necessary and with the minimum level of force necessary to control the situation." It then goes on to say that "You should be aware that using an 'unreasonable level of force' to detain a person could result in a civil lawsuit filed against you. An 'unreasonable level of force' is defined as the level of force that is not appropriate to control a situation." [26] This is quite confusing and could condition a PSO to err on the side of not acting until things get out of control. Since all PSO's are required to carry handcuffs, be armed, have pepper spray and a baton, what are FPS' expectations as to how a PSO should and can act in a violent situation?

Even in an "active shooter" situation, FPS instructions as to what a PSO can do if there is an active shooter in the facility -- but not in the PSO's line of sight --are confusing. For other agencies such as DoE, the policy

[25] FPS SGIM, Chapter 3.2 Common Offenses.

[26] FPS SGIM Chapter 3.6 Detainment Authority

is essentially not to let the threat continue. In some remote FPS protected facilities, it could be a long time before law enforcement arrives. PSO's should not be restrained by confusing and conflicting FPS policies and fear of lawsuits and contract violations when faced with a dangerous or potentially dangerous situation. [27] In situations such as active shooter, FPS needs to instill in security contractors and PSO's a sense that if the PSO engages, the FPS will support their efforts. FPS has stated that the new SGIM (SMART Book) is a "version control document" that can be reviewed and revised more easily, it is likely the instructions for active shooter scenarios and detaining individuals are areas that security contractors and FPS will need to work on.

Another possible strategy for dealing with active shooter and violent/criminal situations is for DHS to authorize PSO's to make arrests. Other federal agencies, such as Department of Energy, under federal statutory authority, authorize their contract security officers to make arrests for certain crimes committed in their presence or if they reasonably believe such a crime was committed. [28] The Homeland Security Act provides for similar arrest authority to be given to employees of DHS "to make arrests without a warrant for any offense against the United States committed in the presence of the officer or agent or for any felony cognizable under the laws of the United States if the officer or agent has reasonable grounds to believe that the person to be arrested has committed or is committing a felony."[29] This section could be amended by Congress to provide such authority to PSO's. If PSO's were given arrest authority (and expected to use it) additional training would be required. However, providing PSO's with arrest authority --- or at the very least not restricting PSO's from exercising arrest authority they may have under some state statutes --- could lead to faster containment of dangerous situations at federal facilities.

Screener Training

The problems that FPS has had with providing PSO's with initial X-ray and Magnetometer training are well documented and FPS is still struggling to get all PSO's the required training. At the same time FPS is transitioning to a new 16 hour initial PSO training and adding an 8 hour annual refresher training. FPS has had to train its personnel to provide this new training and while some contractors are now receiving the new 8 hour refresher training, the 16 hour initial training is still lagging. As mentioned frequently, one solution to address the lack of FPS training resources is to turn over the training to the security

---

[27] For instance, PSO's are sometimes required to pat down individuals and if something is found the individual is asked to remove it. However, in cases where the individual refuses, there is no guidance. Also, FPS officials in the field are giving PSO's detention instructions that differ from what is in the SGIM.

[28] For DoE, arrest authority is provided to contract security officers under 10 CFR 1047 - LIMITED ARREST AUTHORITY AND USE OF FORCE BY PROTECTIVE FORCE OFFICERS. Arrest is defined as any act, including taking, seizing or detaining of a person, that indicates an intention to take a person into custody and that subjects the person to the control of the person making the arrest. http://www.gpo.gov/fdsys/pkg/CFR-2012-title10-vol4/pdf/CFR-2012-title10-vol4-part1047.pdf The U.S. Marshall Services, deputizes its Court Security Officers giving them full law enforcement authority. http://www.usmarshals.gov/duties/ However, CSO's are required to have a law enforcement background or law enforcement training (but this can be a double edged sword).

[29] 40 U.S.C. § 1315 : US Code - Section 1315: Law enforcement authority of Secretary of Homeland Security for protection of public property http://codes.lp.findlaw.com/uscode/40/I/13/1315#sthash.saToUhla.dpuf

contractors who are already supplying around 90% of all PSO training. Security contractors have dedicated trainers while FPS trainers are those same FPS inspectors doing FSA's, acting as COR's, doing patrols, etc.). Security contractor provided will be both more effective and efficient. Delaying PSO's from being able to assume a post because they are waiting on FPS training is not good for anyone, and permitting PSO's to assume posts without the training is a potential safety threat. FPS understands these arguments and has been working with NASCO to initiate a pilot program that will have security contractor instructors be given the training to teach PSO's the screener training. Currently four contracts are being modified to fund this security contractor instructor training and the subsequent 16 hour PSO screener training. In addition, training will be provided to PSO supervisors on the contracts for better quality control. This pilot should get underway early next year. While it has been a long time coming, it represents a sea change in FPS' attitudes toward training and is a milestone in FPS and contractor relations.

When the more expensive 16 hour training does become available, FPS should not unduly restrict the number of the PSO's that can receive the training (and thus be assigned to a screening post) in order to recoup the added costs of the training. FPS must realize that PSO's are often rotated (in some cases as a requirement of the FPS contract) and PSO's doing screening need to be regularly relieved to prevent "going blind" from looking at the x-ray machine too long. There are other situations and reasons why more PSO's will need screening. However, while FPS should not set a number or criterion that will lead to a lack of necessary trained PSO's, at the same time, it would be problematic for FPS to just leave it up to contract bidders to provide FPS with a number of PSO's in their bid that they think need to be given the training for the contract requirements. Based on experience, it is highly unlikely that FPS bid evaluators have the expertise and knowledge of the facilities/hours/rotational requirement/and other factors that are necessary to determine what is the necessary/sufficient amount of PSO's that need to be trained to effectively and safely satisfy the contract requirement. If FPS just leaves it to the bidders, this could lead to FPS selecting a bid that because of an insufficient amount of screening training costs included in the bid, the bid is given an elevated evaluation based on this screener trainer price differential.

Standardized Training and Certified Trainers

FPS is also working on an initiative with NASCO to review, revise and standardize the PSO Training (Lesson Plans) in a new and better format. FPS contractors through NASCO have provided FPS with various contractor PSO training lesson plans and FPS is pulling "best practices" from the plans and "cross walking" them against the new SMART Book at the ISC Armed Security Officer Standard. FPS will then work internally and with contractor to develop a draft national lesson plan for review. The lesson plan though needs to be able to incorporate training for new and developing threats and could have elements that are performance based instead of time based.

FPS also needs to consider ways to improve refresher training. At FPS a PSO's initial training (132 hours) never expires and the refresher training requirement is currently 40 hours every three years. Other agencies provide more initial training and provide substantially more refresher training. FPS needs more refresher training (perhaps 24 hours annually) and should consider at least one annual scenario drill run on site during off hours. These active drills, similar to force on force training currently executed at DoE sites nationally, keep the skills already provided to the contract security personnel fresh and allow for

better and safer weapons handling skills. These additional hours of refresher training and active drills will allow PSO's to learn from and immediately be adjusted for any minor corrections in tactics or technique that will then be perfected for use during a time of emergency such as an active shooter situation.

On a related issue, NASCO fully supports FPS certifying security contractor instructors to provide all the PSO training (not just the screener training as will be done via the pilot program and some of the current certifications). The 2013 ISC "Best Practices for Armed Security Officers in Federal Facilities" recommends that certified trainers provide most of the training for armed security officers (including PSO's).[30] Already numerous state governments "certify" private trainers to provide the required security officer training (firearms, handcuff, baton, "pepper spray") that they require for security officers to obtain state licenses and certifications. Also other federal agencies such as NASA and DoE require security officer instructors to be certified. This would provide for greater confidence in and consistency of PSO training. In its September Report, GAO recommended that FPS security contractor instructors "be certified to teach basic and refresher training courses to guards and evaluate whether a standardized instructor certification process should be implemented."[31] FPS concurred and it envisions using a standardized lesson plan being taught by certified instructors. NASCO stands ready to work with FPS to reach this vision in a timely manner.

PSO Drills and Testing

An important part of keeping a security workforce sharp to conduct regular drills and scenario testing. FPS, through its Operation Shield, conducts penetration tests at federal facilities that test PSO's ability to detect prohibited items. Often, FPS will provide remedial on the spot training during these exercises. However, a persistent problem related to these tests is that FPS is unwilling or does not in a timely fashion, share the results of the Operation Shield exercises with the security contractors. This makes it difficult to determine which PSO's were posted at the time, the conditions, and other information that can be helpful to the security contractor to take corrective and remedial action.

FPS security contractors too have the ability to perform their own penetration exercises of PSO's which are very productive. In these cases, with prior notice to the Government, a company can test a PSO's ability to identify weapons or contraband being introduced to the facility. While Operation Shield exercises by FPS are excellent testing tools, PSO's need to use their skills or they will degrade and FPS testing them in the field infrequently is less valuable than allowing the company to test them more frequently. FPS security contractors conduct such drills with their security officers at other federal agencies and such drills are encouraged by those agencies. However, FPS is inconsistent on allowing security contractor drills and the policies vary by region to region, COR to COR. There does seem to be valid arguments against allowing, under set FPS parameter, security contractors to conduct drills on their PSO's and NASCO supports FPS revisions on this policy to allow for more security contractor drills.

---

[30] Chapter 6.4 Providing Armed Security Officer Training. "All training, whether required or as a refresher, should be done with a certified trainer and/or training organization for: Defensive Tactics, Empty Hand Control Techniques, Firearms (Initial and Requalification Training), Handcuffing Techniques Intermediate Weapons/Compliance, and Use of Force."
ISC Best Practices for Armed Security Officers 2013
[31] See Footnote 3.

Information Sharing and Coordination with Local Law Enforcement

There can be better sharing of threat and risk information between FPS and security contractors. FPS does not share FSA's with contractors providing security for that facility. As to threat information, while FPS has considered utilizing the Homeland Security Information Network (HSIN) to provide alerts, bulletins and critical information to contractors on a timely basis, this has not produced much in terms of effective threat information sharing. Most information that is shared with contractors such as BOLO's and wanted notices, do not make it down to the PSO level. Additionally, FPS also does involve security contractors in the identification and prioritization of threats, thereby losing their potentially valuable input and preventing valuable information from being distributed to PSO's in the field.

Further, FPS Law Enforcement Personnel do not train with the PSOs and do not typically invite local LE to participate in training. Therefore, when a large scale incident or emergency event such as an active shooting does occur, it is unclear how anyone will react. Responsible parties have not discussed action plans in advance and drilled with all the appropriate security/law enforcement stakeholders who would necessarily respond. This leads to confusion during an incident, the worst possible time to have a breakdown in communications. The simple solution is to have more and better communications between the contract security providers and their federal/local law enforcement colleagues.

With less than 1000 FPS law enforcement personnel and thousands of buildings to protect, it is very important that FPS has good coordination with local law enforcement authorities who may be called by PSO to a respond to an incident at a federal facility, and FPS should also include the security contractor in this coordination.

Federalization of Security Officers is Not the Answer

Some have suggested that the solution to improving PSO performance and providing better security at federal facilities is to "federalize" the majority of FPS PSO's (who are stationed at Level III and Level IV facilities). This notion is not only cost-prohibitive but also completely lacking in performance based support for this notion. In response to a question at a hearing before this Committee on FPS in 2009, then FPS Director Gary Shenkel estimated that on an annualized cost basis (thus not including retirement benefits) federalizing FPS security officers would increase costs by about 35% or an extra $400M per year.[32] In terms of performance, a 2011 GAO Report that looked at federal agency use of federal security officers and contract security officers found no differences in performance (but found that using federal officers was more expensive and provided less personnel flexibility and more difficulty in disciplining non-performing officers). [33] Finally, one can look at the current performance problems of the federalized TSA screener force (and performance comparisons done with non-federalized airport screeners) and it abundantly clear that the "federalization" is not the prescription for better screening performance. What is clear though about "federalization" is that it would greatly increase the costs to FPS.

[32] Hearing before the Senate HSGAC "The Federal Protective Service: Time for Reform" April 19, 2009.
[33] GAO: FEDERAL FACILITY SECURITY: Staffing Approaches Used by Selected Agencies GAO-11-601 June 2011. http://www.gao.gov/assets/330/320625.pdf

Conclusion

Federal facility security is a multi-layered operation involving common standards as well as unique requirements. In order to increase the level of security provided at federal facilities in a cost-effective manner, Federal agencies and their security providers like FPS, need to work better and smarter together in assessing risks, discussing risks and countermeasures, and then implementing countermeasures. One important countermeasure is the use of contract security officers. Contract security officers are the front line forces in the protection of federal facilities and they often bear the initial brunt and/or provide the initial reaction to an active shooter incident. In the 2009 Holocaust shooting, upon entering the Museum the shooter shot and killed a contract security officer but then the shooter was shot and disabled by another contract security officer. There is no doubt that well trained contract security officers can be an important part of any facility security plan. FPS, as the largest supplier of contract security to the federal government, is definitely making progress in improving this element of the security service it provides to federal agencies. There continue to be issues with the Protective Security Officer Program, but under the direction of Director Patterson, working with his contract security partners, FPS is actively addressing these issues. Importantly, every element of the Program is subject to potential review and revision if necessary. New ways are being found to provide better training, including working with other agencies, and FPS' oversight and review processes are being reformed to provide for better quality management. All of these efforts will increase the performance and effectiveness of the FPS contract security force.

Some of the needed changes and improvements to the PSOP (such as more training) or the need to deploy more PSO's at a facility will likely require additional funding and FPS must explain to its federal clients why these increases are necessary but in the final federal facility security equation, federal tenants must not be allowed assume unreasonable risk because of budget concerns or because of a lack of understanding.

Background on NASCO and Private Security

NASCO is the nation's largest contract security trade association, whose member companies employ more than 300,000 security officers across the nation who are servicing commercial and governmental clients, including providing security officers to numerous federal agencies for the protection of federal facilities. NASCO also has a "Government Security Contractors Caucus" that includes non-NASCO members and focuses on federal security contracting programs, such as FPS. Formed in 1972, NASCO strives to increase awareness and understanding among policy-makers, consumers, the media and the general public of the important role of private security in safeguarding persons and property. At the same time, NASCO has been the leading advocate for raising standards for the licensing of private security firms and the registration, screening and training of security officers, and NASCO has worked with legislators and officials at every level of government to put in place higher standards for companies and officers.

At the federal level, NASCO was the driving force behind the 2004 passage of the Private Security Officers Employment Authorization Act (PSOEAA), which authorized all employers of private security officers to request FBI criminal background checks on their officers, and NASCO is continuing to work to establish an effective and comprehensive PSOEAA check process. Of more relevance to today's hearing, as mentioned in the introduction, since 2007 NASCO has worked closely with both the House and the Senate Homeland Security Committees (appearing at three House hearing), the Federal Protective Service (FPS) and the Government Accountability Office (GAO) on issues and legislation related to FPS.

Nearly 2 million people are employed in private security domestically compared to fewer than 700,000 public law enforcement personnel. Approximately 75 percent of private security personnel work for contract security companies, with the balance serving as proprietary or "in-house" security. The vast majority of contract security firms employ many former law enforcement and military personnel in management and as security officers. Private security officers are often the "first" responder on the scene of a security or terrorism-related incident providing crucial support to public law enforcement. In addition, with increasing fiscal pressure on governmental entities, private security is increasingly relied upon to fill the gaps resulting from law enforcement funding cutbacks.

**Written Testimony of AFGE Local 918- Federal Protective Service Union President David L. Wright before the Senate Homeland Security and Governmental Affairs Committee on December 17, 2013:**

**The Navy Yard Tragedy: Examining Physical Security for Federal Facilities**

Chairman Carper, Ranking Member Coburn and Members of the Committee:

Federal employees and facilities are very vulnerable to attack from both criminal and terrorist threats. We are all appalled at the Navy Yard tragedy. However, the Navy Yard, like other DOD Installations, is better protected than most federal facilities across the nation because they use a mix of armed federal and private security onsite, or use only federal and military personnel.

In the 7 years since the Union demanded reform aimed at efficiently and effectively accomplishing the FPS Mission, there have been numerous GAO reports critical of the Federal Protective Service, numerous Congressional hearings promising reform and enough incidents at federal buildings to shock Congress and the public into demanding reform. Yet little progress has been made in the reform of this critical Homeland Security agency. Should a tragedy like the Navy Yard shooting occur at a federal building secured by the FPS, many in government will have to answer for the inaction.

1. **FPS Law Enforcement Personnel Active Shooter Training and Preparedness.** FPS Police Officers and Inspectors are fully trained and equipped to respond to Active Shooter incidents in Federal facilities – in the cities where we are sufficiently manned. FPS Law Enforcement recruits are extensively trained at Federal Law Enforcement Training Center (FLETC) in classroom and scenario based training. Recurring classroom and scenario based

training for each Law Enforcement Officer occurs annually in the Regions and every five years in Advance Law Enforcement Refresher Training (ALERT). As you may deduce from accounts of the Navy Yard shooting – many in FPS responded to the scene quickly. But much like the Capitol Police – FPS was disallowed to participate in the tracking of the suspect due to jurisdictional concerns – as the Navy Yard is not a "GSA –controlled facility". As the National Capital Region (NCR) FPS HQ is barely two minutes from the Navy Yard – an expeditious FPS response was available but unused due to bureaucratic limitations. Additionally, FPS capabilities to respond to potential chemical and biological attacks at federal facilities – once a thriving program - has been all but eliminated by a management staff that apparently see such response as the purview of local authorities.

**2. Vulnerability and threats.** Federal buildings face serious threats and vulnerabilities:

Federal buildings are open to the public and are natural targets for individuals or groups who feel wronged by the Government. Some agencies, such as SSA and IRS, frequently receive threats from individuals, many of whom are emotionally disturbed. The Federal Facility Threat Picture, a FOUO document published quarterly by FPS, summarizes these threats. Others are attractive targets because of their mission criticality; threats to tenant agencies; size; and population - and thus are deemed medium or high risk (Facility Security Levels 3 & 4).

Decisions to implement or not implement FPS security countermeasure recommendations are made by Facility Security Committees (FSC's) at individual facilities. FSC's are comprised of a representative from each tenant federal agency. Many of the FSC members are non –security professionals assuming the FSC membership as a collateral duty. Tenant Agency lack of compliance with the ISC Physical Security Criteria also make facilities vulnerable. If FPS

recommended countermeasures are not accepted, the FSC's should recognize "acceptance of risk", but as noted in a memorandum from the Administrative Office of US Courts on November 22, 2013 "There is **no** ISC requirement that individual FSC members sign a document "accepting risk." Rather, the ISC standard is that if a proposal is voted down, it will be **noted** in the meeting minutes." This includes FSC decisions to have an install alarm or CCTV systems, which non - law enforcement employees are allowed to bypass screening for weapons and explosives, and other common sense protective measures. Additionally, the tenants in a building must pay FPS or GSA for any security countermeasures, so agency budget and individual FSC member's lack of authority to commit funding often becomes the only or most important factor in these decisions.

Unlike this Senate and other Capitol buildings where the weapons screening force is comprised of Federal Police Officers, every one of the 1.4 million federal employees and visitors who use GSA -owned or leased facilities must rely on private sector contract guards for this function. These contract guards are beholden to state and local licensing restrictions and sometimes significant limits on authority. These guards are selected, trained, employed and supervised by private companies whose escalating wage rates during the contract period are paid by the government. Guards who violate contract terms are often only moved from one federal security post assignment to another since discipline is up to the private employer - retraining guards or hiring and training new guards eats into company profits. Even when malfeasance is detected, such as a case where a guard company employee falsified guard training records, it is treated as rogue behavior by an employee that the company can't control. The services from the company continue on that and other contracts with only that corporate employee debarred. The GAO recently highlighted serious significant issues with guard training and monitoring that included

contracts where guards had received no training on active shooter incidents and many cases where guards operating x-rays and magnetometers had not been trained to higher standards in detection of weapons and explosives.

Federal Police Officers at Senate and Capitol buildings are a proven cost-effective measure – how can we not provide the same protection at major GSA –controlled buildings with several hundred federal employees? Federal Police Officers at the entrance here are fully trained on the magnetometer and x-ray they operate – how can we demand less at all buildings? The Federal Officers at this building have the duty and authority to respond to active shooters – how can we demand less at federal buildings with thousands of occupants? Federal Police Officers are trained at the Federal Law Enforcement Training Center (FLETC) and are obligated in their lawful assigned duties to respond on behalf of the visitors, employees and federal property that they are assigned to protect.

**3. Federal Protective Service mission and staff duties.** FPS provides a safe workplace for federal employees and secure facilities for these employees and members of the public who seek services in the over 9,000 GSA facilities nationwide. Public Law requires FPS have a minimum of 1,371 total staff (down from 1,475 in FY07), of which 1,003 must be in-service field law enforcement staff. FPS also uses over 580 support contractors not involved in guard oversight. We accomplish the mission primarily through our Inspector workforce who are Federal Law Enforcement Officers also trained as Physical Security Specialists and assigned a portfolio of buildings. In addition to Inspectors there are Police Officers (being phased out through attrition), Explosive Detection Team Canine Handlers, Special Agents and Personnel Security Specialists who deliver primary services. There are also supervisors, program managers and mission support staff to perform management and support activities.

As law enforcement officers, the less than 650 Inspectors and legacy police officers respond to over 30,000 incidents a year, make over 1,900 arrests and conduct over 13,000 explosive K-9 sweeps in addition to community police/ physical security duties for their assigned buildings.

On average, each inspector who is not a K-9 handler has about 23 buildings and for each:

- Performs a Facility Security Assessment (FSA) either every three or five years based on the facility security level;
- Recommends security countermeasures such as alarms, CCTV, blast mitigation and contract guards (including estimated costs) as well as security practices and procedures such as entry control for employees and visitors, facility security plans and hours contract guard posts should be staffed based on the ISC Physical Security Criteria and threat assessments developed by FPS Special Agents;
- Presents and coordinates FSA recommendations for approval by Facility Security Committees (FSC) consisting of all tenant agencies;
- Participates in FSC meetings conducted at least annually to update facility occupants on law enforcement efforts and security measure effectiveness;
- Assists FSC in the development and exercise of emergency plans covering tenant actions to situations that range from fires and earthquakes to explosive attacks or active shooter;
- Recommends and conducts training for tenants on reaction to and prevention of undesirable events such as procedures to respond to an active shooter;
- Drafts and updates post orders to provide detailed instructions to contract guards;
- Participates in operation shields, marketed as providing a highly visible law enforcement presence with three or more Inspectors for at least an hour;

- Testing/ checks of countermeasures (i.e. alarms, CCTV) to ensure they are functioning properly when conducting an assessment and during some operation shields; and
- Conducts proactive police patrol to detect and deter threats to a facility as well as identify and mitigate opportunities for criminal or terrorist attack.

Inspectors and Police Officers also perform contract guard monitoring duties that include:

- Inspections of contract guard posts with a frequency based on the facility security level to ensure they are present for the correct times, understand the facility and follow the contract including specific orders/ instructions for that post;
- Compliance monitoring of contract guard initial training and refresher training ;
- Attendance to observe and document every FPS required contract guard firearms qualification (twice a year for most guards);
- Conduct eight hours of initial training for each new contract guard; and
- Conduct at least eight hours of weapons detection training for each guard.

Approximately 80 Special Agents investigate crimes and provide intelligence including:

- Conduct investigations of complex or serious crimes at federal facilities;
- Investigate and follow up with individuals who make threats to federal employees and facilities (except for threats to the Judiciary which are the purview of the USMS);
- Complete the threat portion of FSA;
- Conduct covert testing of contract guards and other facility countermeasures;
- Regional Intelligence Agents coordinate and disseminate threat information; and
- Serve on FBI Joint Terrorism Task Force (JTTF) to ensure awareness of threat information regarding federal facilities.

Personnel Security Specialists using criminal records and OPM investigations, annually adjudicate about 35,000 FPS contract guards and GSA building service contractors (i.e. building maintenance or construction workers) to ensure they meet suitability standards.

Inspectors and Police Officers are assigned to Area Commands which are responsible for a geographic area such as a large city (i.e. Cleveland), portion of a major city (i.e. Kansas City has two; DC about 10), or sometimes an entire state. Area Commands report to a District Commander. There are approximately 120 Areas and Districts. Districts report to one of 11 Regions. Regions have Program Managers for guards and security assessments; and Threat Branch (Special Agents); Risk Management and Mission Support branches. Regions report to one of three newly created Assistant Directors for Field Operations (ADFO).

**4. FPS Contract Guards.** FPS uses approximately 12,000 contract guards (called Protective Security Officers or PSO) to perform patrol & response; personnel, package, and vehicle screening; alarm and CCTV monitoring; and access & visitor control duties at buildings. Each post is typically recommended in a FSA based on the ISC Physical Security Criteria. FSC's approve the post and the hours it is staffed. The guard services for a building are funded based on the space each agency occupies. Specific services inside a tenant's space are provided to deter disruptive behavior in some offices (i.e. IRS and SSA) and are paid by that tenant. FPS procures, manages and monitors these services with some exceptions such as Judicial Space where contract guards (called Court Security Officers or CSO's) are procured and managed by the U.S. Marshals Service.

FPS has over 110 guard contracts. Each contract usually covers a portion of a state, the whole state or several states except in the NCR where the service areas are individual buildings rather

than a contiguous area. For example in my home region there is one contract which covers all four states. The entire state of Illinois is serviced through one contract. Conversely in the NCR there are over 40 contracts, so an Inspector with buildings in a ten block area could have three or more different contractors servicing those buildings. I have been told it is impossible to consolidate contracts to fixed geographic areas in NCR and replicate the reduced workload noticed in my home region due to small business set asides and other Federal Acquisition Regulation (FAR) issues. Given those rules I can understand why Congress uses Federal Police Officers instead of contract guards to protect Capitol facilities– it would be an impractical arrangement for the Capitol Police to manage one private guard company in the Hart Senate Building and another in the Dirksen Senate Building.

**5. FPS Funding.** FPS is often described as a "fee -funded" organization. But unlike CIS, TSA or CBP where the public using their services pay the fees, FPS collects only from other federal agencies using GSA -owned or leased facilities. It does this through three security charges. The first is a basic security charge which much like a local property tax is designed to pay for general law enforcement and security services. The second is a building specific security charge based on services provided to specific buildings and includes contract guard services as well as security systems (i.e. alarms and CCTV). The third is security work authorizations where individual tenants pay for guard services and security systems within their space such as guards in SSA and IRS offices. Additionally all tenant agencies pay GSA either in the rent bill for leased space or as an addition to the rent bill in owned space, for fixtures such as access control systems, bollards and blast mitigation. Security in this building is not based on the ability of an individual Senate Office's ability to pay – why should other federal facilities be different?

**6. Mission Performance.** How well are the 740 or so boots on the ground Inspectors, legacy Police Officers and Special Agents doing at providing the critical law enforcement and security services to buildings FPS protects? Overall, quite well given the dynamic mission, HQ staff with little to no law enforcement field experience and inadequate numbers of Full Time Employees (FTE). How is FPS management doing? Not so well.

- Law Enforcement Response – Inspectors and Police Officers report challenges in responding to calls for service. Many tenants call local police because FPS does not have sufficient resources due to staffing and facility security tasks and is only on duty in most places for 8 to 10 hours weekdays. I would grade this area a B+ for times Inspectors and Police Officers are on duty.
- Facility Security Assessments -- Inspectors report the interim vulnerability assessment tool works okay as they become more familiar with it – but still cumbersome due to widely uneven application by Regional and mid –level managers. Inspectors are concerned it does not align well with the ISC security criteria and misses several countermeasures; that only a baseline level of protection is computed while the ISC requires a customized level of protection; threat levels are from the nationwide Design Basis Threat rather than a specific building; and well informed FSC's expect the deliverables in the ISC standards which are higher than MIST provides. Some tenants ask about the lack of consequence consideration, but most are more concerned that recommendations be tailored to their facilities' threats. Overall tenants appear satisfied and understand the recommendations. Based on these reports, I would grade this area a C+.

- Emergency and Security plans -- Inspectors report they simply don't have time to work with facilities on emergency and security plans particularly in buildings with government and commercial tenants that require greater coordination. Much of this work is pushed to tenant staff to the detriment of those agencies' primary missions. I would grade this area a C+ since the work is getting done but FPS duties are pushed to tenant staff.
- Tenant Training – Inspectors are very concerned FPS does not adequately deliver training for active shooter to tenants. There have been several sessions where local police participated but fully integrated training both for responders and those in a facility are critical to reduce the tragic consequences inherent in active shooter incidents. I would grade this area a C; FPS can provide updated information but practice is critical. We have a fire drill in every facility each year, why can't we do the same for active shooter reaction?
- Proactive Patrol – Patrol is critical to detect and deter threats as well as to recognize when operational or other countermeasures are not working. FPS randomly conducts "Operation Shield" but during FY 13 there were only 1,141 at 460 buildings nationwide. There were 8,600 field interviews conducted with only 103 citations, arrests or opening of investigation. Inspectors report regular unannounced proactive patrols by individual or pairs of officers are much more likely to provide an acceptable level of detection and deterrence than a miniscule 1.2% arrest rate. I grade this as a B for effort and give management a D for results. Buildings on Capitol Hill benefit from extensive proactive patrol from the Capitol Police; why shouldn't all large facilities have the same benefit?

- Investigations – Special Agents report the scenarios eligible for use on covert tests of guards have been reduced and limit the ability to fully assess guard performance. I give FPS management a D for not using the full range of tests.
- Contract Guard Oversight – In October GAO reported continued failure to ensure guards are properly trained. That being said, in some Regions all guards receive FPS training, untrained guards are never used at a screening post, guard firearms qualification is fully monitored and guards are trained on active shooter at the facility they protect. This happens because dedicated FPS Inspectors work overtime to ensure contract guards are trained to prevent weapons from entering facilities and are properly qualified on their weapon. They live the mission of keeping federal employees and facilities safe and simply refuse to fail. I make no excuse for supervisors and senior managers in many Regions who fail to ensure proper training. These problems could have been fixed. Three years later they obviously should have been fixed, and the managers who failed should be held accountable. I grade management at HQ, and in the deficient regions and districts with an F. The Inspectors who refused to fail and their managers get an A.
- Facility Security Committees – Clearly the current structure is broken on decisions to implement pbysical security countermeasures and documenting risk acceptance. If the Administrative Office of the Courts don't take risk acceptance seriously almost no one will. I would grade this area a D.
- Security Funding – The current method of moving money within the Government to pay for critical law enforcement and security to protect employees and facilities is inefficient since it implements countermeasures such as armed guards based on an agencies' ability to pay - not actual risk. I grade funding a D.

- Staffing – Although I am not privy to exact staffing data, our research shows that 270 employees and over 350 contractors are assigned to FPS HQ. The Inspectors, Police Officers and Special Agents who perform our direct services comprise only 54% of the staff, with law enforcement supervisors another 9%. Thus only 63% of the staff engage in or directly supervise law enforcement/security at buildings. I'm not a management expert but almost 20% of personnel and 55% of support contractors assigned to the HQ "supporting" 11 largely self-sustaining regions seems out of kilter. I shouldn't be surprised, since the HQ contracting staff increases based on the cost of the contracts and guard wage rates they negotiate. According to our research, it is clear that FPS has about 920 in-service field law enforcement staff including numerous Regional staff who do not respond to calls for service or perform facility security assessments. It appears that FPS may not have quite reached the goal of complying with the law that requires over 1,000 field level law enforcement. 80 or more additional Police Officers would greatly improve service delivery. I give management a D for staffing HQ instead of more Police Officers and Inspectors to physically protect facilities.
- Duplicative Security Staff in Federal Agencies: Federal agency Security Directors naturally want complete control of all aspects of security just as agencies want to own and lease their own office space regardless of efficiency. Some security staff such as the DHS Office of Security and ICE Security Management Unit even armed their security specialists using 40 USC 1315. They do not have a law enforcement role and their use as such is inefficient; the same goes for the size of security staff at many agencies some of whose staff duplicates services provided by FPS. I give these agencies a C- for diminishing their mission resources.

7. **Improvement Recommendations.**

- **Law Enforcement Response to include Active Shooter and Chemical/Biological Attack Response** –Recommend hiring and reinvigoration of the GS-083 Federal Police Officer workforce in major cities to ensure adequate response to criminal incidents. Remove all bureaucratic obstacles to FPS response to Active Shooter situations – if life is endangered at a Federal property – FPS law enforcement officers should respond as equipped, trained and available. Reinvigorate the FPS Hazardous Materials Response Plan and workforce.
- Facility Security Assessments – Remove FPS from the (to date) unsuccessful business of creating an ISC –compliant FSA tool. Recommend that DHS create the ISC –compliant FSA tool that would ensure the more cost effective custom level of protection rather than the baseline driven only by the general facility security level.
- Emergency and Security plans -- We can't keep pushing our work onto agencies – FPS has the security mission and it should execute it across the nation with increased resources and manpower.
- Tenant Training –We have a fire drill in every facility each year, why can't we do the same for active shooter reaction?
- Proactive Patrol – Routine proactive patrol at FSL 3 and 4 buildings.
- Investigations – Use the full range of covert test scenarios.
- Contract Guard Oversight – Establish clear requirements that match available resources and hold managers accountable.

- Use of Contract Guards -- Since the use of Federal Police Officers is a cost effective alternative at Senate and Capitol Buildings, it should be the same for large multi-tenant facilities open to the public with a Facility Security Level of 3 or 4. Continue the use of contract guards at small facilities such as SSA, CIS and IRS service offices.
- Facility Security Committees – Recommend required reporting to Congress of which recommended ISC criteria are not implemented. Agency budget considerations for FPS recommended physical security countermeasures should be the purview of that Agency's HQ - not at the field or regional level. Alternatively, FPS as an "honest broker" could be empowered as the authority at the national level to overrule any FSC where too much risk is accepted.
- Security Funding – FPS be funded to implement building specific security based on risk priorities not agencies' ability to pay.
- Staffing -- Recommend starting with the FY 07 FTE of 1,475 which provided better and effective service before OMB, whose offices are protected by the Secret Service, cut the protection provided to other federal employees. Make NPPD fund its own support (i.e. Human Capital) from its budget instead of sucking up more than 30 FPS FTE who really don't work for FPS. Mandate efficient HQ operations by transferring at least 3 of the 8 SES to areas in DHS that really need them. Raise and enforce the in-service field staff minimum to 1,140.

Can FPS do better? Absolutely! Performance across the board can improve with focused professional and ethical management that builds on best practices in the regions -- give our Inspectors tools that work and direction on priorities and they will make sure these issues are

fixed. What has not worked is lack of clear direction funneled through extra layers of ineffective, scattered management and new bureaucracies.

In summary, as AFGE President J. David Cox recently stated while calling on federal agencies to review their operational procedures to ensure the safety and security of all federal employees "Federal employees are on the front lines in delivering services to the American people and oftentimes that puts them in harm's way." These employees and the public they serve deserve the best and most effective protection we can provide.

FOR INTERNAL USE ONLY

November 22, 2013

**TO:** **FPS HQ**

**FROM:** **Deputy Director of Operations Kris Cline**

**SUBJECT:** **Active Shooter Update**

FPS Law Enforcement Colleagues,

As we reflect on recent active shooter incidents we are reminded of the dramatic increase in these types of events over the last five years. These incidents are always unique, dangerous and extremely dynamic and underscore the critical importance of your vigilance every day.

Each of you provide a level of safety, security, protection and simply a sense of well-being to thousands of federal employees who work in and visitors who enter our facilities. You respond to thousands of calls for service, deliver hundreds of hours of training, coordinate and participate in occupant emergency drills, assess vulnerabilities, and conduct investigations and inspections for our tenants to prepare them for just such an event.

You have received extensive Active Shooter training at AITP and ALERT and have been provided tools and resources to prepare you to react to an Active Shooter incident.

Of critical importance is the role of the Protective Security Officer (PSO) during an Active Shooter incident. PSOs are typically the first person encountered when someone enters one of our facilities. PSOs receive instruction during their initial and refresher training on what actions to take during "special situations" - which may include events such as building fires, active shooter or identification of suspicious packages. However, in light of the dramatic increase in active shooter events, and the dangerous and extremely dynamic nature of such incidents, it is critical that the instruction on this topic be reiterated and reinforced so that every PSO fully understands the proper response procedure.

To this end, the following information has been provided to our PSO vendors to be disseminated to every PSO employed in support of a Federal Protective Service (FPS) contract.

Enclosure (1) Active Shooter Instructions

Note: This information will be added to all post orders along with any additional requirements on a post-specific basis. This information shall be incorporated into any active shooter awareness guidance or training.

When faced with an active shooter situation or situation where a person brandishes a firearm and/or otherwise threatens the PSO or others in a federal building or on federal property, PSOs will take the following actions and due to the unique circumstances of such situations, PSOs may take these actions in a different order than listed:

- PSOs will defend themselves and protect others as necessary in compliance with their contractually required use of force training and applicable state law
- Immediately notify the MegaCenter and follow the emergency notification instructions in the post orders
- Relay the following information, if known:
  - Description of the event
  - Suspect(s) location
  - Suspect(s) description
  - Weapons used/carried
  - Description of any device carried or used by the suspect(s)
  - Suspect(s) direction of travel
  - Number and location of casualties and assistance needed
  - Number of friendly by-standers secured at your location
- PSOs will maintain their assigned posts and follow post orders to the maximum extent practicable or until directed otherwise by responding law enforcement personnel; this is critical to facilitate evacuation and prevent more potential victims from entering the danger area(s)
- Direct the building occupants in accordance with the Occupant Emergency Plan
- Secure all entrances
- If the shooter is outside, do not let the tenants and visitors go outside
- Stay out of the view of the doors and windows to the extent possible
- Turn off the lights and close the shades/ curtains, if possible
- PSOs are not trained in response tactics such as those critical to a contact or rescue team but in an active shooter situation, PSOs must comply with directions given by the law enforcement authority responding to the threat.

PSOs are reminded to:

- Be vigilant while conducting patrols and dealing with the public
- Be aware of surroundings at all times and remain alert for suspicious activity
- Be aware of individuals that appear to be out of place (clothing, exhibit apprehension, nervousness, etc.) and report as appropriate
- Continuously review post orders and emergency procedures
- Routinely inspect and test equipment as outlined in the Post Orders
- Ensure exterior entrances are secured as appropriate
- Stop anyone who may be attempting to gain unauthorized access to a secure area and follow procedures in the post orders

**Post-Hearing Questions for the Record**
**Submitted to Caitlin A. Durkovich and L. Eric Patterson**
**From Senator Thomas R. Carper**

**"The Navy Yard Tragedy: Examining Physical Security For Federal Facilities"**

**December 17, 2013**

| | |
|---|---|
| **Question#:** | 1 |
| **Topic:** | status update |
| **Hearing:** | The Navy Yard Tragedy: Examining Physical Security for Federal Facilities |
| **Primary:** | The Honorable Thomas R. Carper |
| **Committee:** | HOMELAND SECURITY (SENATE) |

**Question:** Please provide a status update of the Federal Protective Service's progress implementing each of the Government Accountability Office's (GAO) recommendations for the agency. For any "open" recommendation, please provide a timeline and details for the agency's plans to implement that recommendation.

**Response:** Between January 2004 and December 2013, the Government Accountability Office (GAO) issued 52 recommendations to the Federal Protective Service (FPS). By the end of calendar year 2013, 22 of those recommendations were closed by GAO and 30 are open. Of the 30 open recommendations, three are awaiting formal closure from GAO to the Department. The timelines and details for the implementation of the 30 open recommendations are included in Attachment 1.

| | |
|---|---|
| **Question#:** | 2 |
| **Topic:** | security measures |
| **Hearing:** | The Navy Yard Tragedy: Examining Physical Security for Federal Facilities |
| **Primary:** | The Honorable Thomas R. Carper |
| **Committee:** | HOMELAND SECURITY (SENATE) |

**Question:** For civilian federal facilities protected by the Federal Protective Service, the chair of a Facility Security Committee is responsible for determining which security measures are implemented. Yet, as GAO has reported, few personnel serving on Facility Security Committees have much education or training in security matters, and they frequently do not follow Federal Protective Service recommendations for security measures because of cost concerns.

Do you believe a minimum level of education or training in security issues should be provided before an individual can serve on a Facility Security Committee? If so, how much?

**Response:** Yes, the Interagency Security Committee (ISC) believes a minimum level of training is needed for all Facility Security Committee members, including the chair. As stated in the *Risk Management Process for Federal Facilities: An Interagency Security Committee Standard (RMP)*, Section D.2.6 Federal employees selected to be members of a Federal Facility Security Committee will be required to successfully complete the ISC online training courses that covers the basics of the ISC RMP. These courses are available on the Homeland Security Information Network and Federal Emergency Management Agency Web sites. The course topics include:

1. IS-890a - Introduction to the Interagency Security Committee;
2. IS-891 - Interagency Security Committee: Facility Security Level Determinations for Federal Facilities (FOUO);
3. IS-892 - Physical Security Criteria for Federal Facilities (FOUO); and
4. IS-893 - Facility Security Committees.

Additionally, the Department of Justice and the ISC, in cooperation with the Office of Personnel Management, offer a classroom course on the ISC RMP as an option for Facility Security Committee members.

**Question:** Who should be responsible for providing that education and training?

**Response:** The ISC is responsible for facilitating the training online; the Facility Security Committee members are responsible for the completion of the training.

**Question:** Defense Department guidelines for military facility security indicate that a lack of funding alone is not a sufficient reason for failing to comply with a facility

| | |
|---|---|
| **Question#:** | 2 |
| **Topic:** | security measures |
| **Hearing:** | The Navy Yard Tragedy: Examining Physical Security for Federal Facilities |
| **Primary:** | The Honorable Thomas R. Carper |
| **Committee:** | HOMELAND SECURITY (SENATE) |

security standard. Do you believe cost alone should be considered a sufficient reason for a Facility Security Committee to decide not to implement a security recommendation made by the Federal Protective Service?

**Response:** Cost, along with other possible rationales for risk acceptance, is an acceptable reason for not implementing a security recommendation made by the Federal Protective Service, but only if the Facility Security Committee:

1) Followed the ISC RMP by first determining the Facility Security Level (FSL) of a facility;
2) Determined risks in the facility;
3) Identified the desired level of protection;
4) Identified the desired level of protection is not achievable;
5) Developed alternatives if possible; and
6) Accept risk only when absolutely necessary.

The *ISC RMP* provides details to implement security recommendations where cost could be an issue in section 5.1.6. Cost effectiveness is based on the investment in the countermeasure versus the value of the asset. In some cases, investment in an expensive countermeasure may not be advisable because the lifecycle of the asset is almost expired. In addition, consideration should be given to whether other countermeasures may take priority for funding. Note that "cost-effective" is a different determination than "cost-prohibitive." A countermeasure is cost-prohibitive if its cost exceeds available funding. Funding may exist for a countermeasure, but it may not be a sound financial decision to expend that money for little gain; thereby eliminating cost-effectiveness.

Cost considerations could also be a primary factor in a decision not to implement a recommended countermeasure or a decision to defer a funding request until such time as the likelihood of obtaining funding is more favorable. The ISC Risk Management Process Standard does not mandate the use of a specific cost analysis methodology. However, all costs, including life-cycle costs, shall be considered in whatever cost analysis methodology is used. In addition to direct project costs, those costs associated with indirect impacts (e.g., business interruption, relocation costs, or road closures) should be considered. Any decision to reject implementation outright or defer implementation due to cost (or other factors) must be documented, including the acceptance of risk.

| | |
|---|---|
| **Question#:** | 3 |
| **Topic:** | direct appropriation |
| **Hearing:** | The Navy Yard Tragedy: Examining Physical Security for Federal Facilities |
| **Primary:** | The Honorable Thomas R. Carper |
| **Committee:** | HOMELAND SECURITY (SENATE) |

**Question:** Do you believe the Federal Protective Service might be more effective if it received a direct appropriation, and could pay for the security measures it recommended, rather than request that tenant agencies pay for those security measures?

**Response:** In FY 2013, FPS developed and delivered an activity-based costing (ABC) model to improve its internal financial management and to more clearly identify the costs to protect Federal facilities and their occupants. The modeling effort identified the costs for FPS to deliver protection services. The model is a strong management tool that enables operational decisions and tradeoffs involving risks associated with the cost and performance of the impacted activities.

| | |
|---|---|
| **Question#:** | 4 |
| **Topic:** | personnel |
| **Hearing:** | The Navy Yard Tragedy: Examining Physical Security for Federal Facilities |
| **Primary:** | The Honorable Thomas R. Carper |
| **Committee:** | HOMELAND SECURITY (SENATE) |

**Question:** At the hearing, GAO noted that Federal Protective Service personnel struggle to keep up with the amount and variety of work expected of them. Do you believe the Federal Protective Service should reexamine its workforce composition? Have you considered convening any working groups or outside experts to explore this matter?

**Response:** FPS's protective mission requires an agile and professional workforce that can respond and be resilient within a dynamic operating environment. FPS's workforce staffing model, which supports the Congressional requirement for an FPS Strategic Human Capital Plan, was developed in collaboration with the Department of Homeland Security (DHS) Federally Funded Research and Development Center Systems Engineering and Development Institute. This model enables FPS to baseline current workforce requirements; assist managers in making staffing and allocation decisions based on available mission data and activity-based work standards; and prioritize the delivery of services to risk and documenting performance relative to risk.

However, staffing requirements are not static and will vary depending on both the nature and level of threat and required capabilities. Accordingly, FPS's baseline staffing model will continue to be refined and improved for use in determining functional gaps, prioritizing those gaps, and making strategic human capital decisions to close those gaps.

| | |
|---|---|
| **Question#:** | 5 |
| **Topic:** | federal guidance |
| **Hearing:** | The Navy Yard Tragedy: Examining Physical Security for Federal Facilities |
| **Primary:** | The Honorable Thomas R. Carper |
| **Committee:** | HOMELAND SECURITY (SENATE) |

**Question:** Director Patterson, in your testimony you indicated that in some states there is a conflict between federal guidance and state laws when it comes to responding to an active shooter. You indicated state laws may constrain a security guard from taking certain actions, such as interdicting an active shooter. However, the National Association of Security Companies has indicated that the Federal Protective Service appears to limit the authority of armed guards protecting federal facilities from active shooters, while some state laws may require armed guards intercede.

What guidance has the Federal Protective Service provided to its armed contract guards with respect to responding to an active shooter?

Please provide a list of states which limit the authority of an armed contract guard to respond to an active shooter. Please also provide a list of any states which may require armed contracts guards to interdict an active shooter.

**Response:** FPS Protective Security Officers (PSO) are not sworn law enforcement officers. Rather, PSOs are employees of private security companies or 'vendors' which are independent contractors doing business with the Federal Government. The relationship between FPS and private-sector vendors is contractual in nature and FPS does not have the authority to deputize PSOs in a law enforcement capacity.

Therefore, an individual PSO's authorities to perform protective services are based on state-specific laws where the PSO is employed. While state-specific laws do not explicitly limit a given PSO's ability to respond to an active shooter situation specifically, in most instances, PSOs rely on the 'private person' laws, also known as 'citizen's arrest' laws, of a given state as well as that state's laws relating to self-defense, defense of others, and use of force to defend property.

The National Protection and Programs Directorate (NPPD) Office of Legislative Affairs welcomes the opportunity to further discuss the list of states limiting armed contract guard's authority during a briefing.

| | |
|---|---|
| **Question#:** | 6 |
| **Topic:** | Interagency Security Committee |
| **Hearing:** | The Navy Yard Tragedy: Examining Physical Security for Federal Facilities |
| **Primary:** | The Honorable Thomas R. Carper |
| **Committee:** | HOMELAND SECURITY (SENATE) |

**Question:** The Executive Order establishing the Interagency Security Committee and empowering it to develop standards for federal facility security also made it responsible for monitoring compliance with those standards. However, the Interagency Security Committee has never monitored compliance, and has required agencies monitor their own compliance.

Do you believe this is lawful and appropriate?

**Response:** We view compliance with ISC policies and recommendations as a critical component of efforts to secure Federal facilities. The President, in Executive Order 12977, assigned all ISC member agencies the responsibilities to "develop a strategy for ensuring compliance with [security] standards" and to "oversee the implementation of appropriate security measures in Federal facilities." In an effort to aid departments and agencies in executing their individual compliance responsibilities, the ISC issued the *Risk Management Process: An Interagency Security Committee Standard (Standard),* which describes the necessary criteria and/or actions that must be taken for Federal facility risk assessment data tools to be validated as compliant with the ISC Standards.

The *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 nonmilitary Federal facilities. The Standard also provides guidance for customization of the countermeasures for Federal facilities.

The *Standard* incorporates and supersedes the previous guidance in the *Facility Security Level Determinations for Federal Facilities: An Interagency Security Committee Standard* published in March 2008, *Physical Security Criteria for Federal Facilities: An Interagency Security Committee Standard* published in April 2010, *Design-Basis Threat: An Interagency Security Committee Report 7th Edition* published in March 2013 (report updated bi-annually), *Facility Security Committees: An Interagency Security Committee Standard, 2nd Edition* published in January 2012, *Child Care Centers Level of Protection Template* published in May 2010, and *Use of Physical Security Performance Measures* published in June 2009.

In order for the ISC to lawfully and appropriately monitor compliance, standards had to be developed to monitor. Over a number of years, the ISC developed the elements now incorporated into the ISC *Risk Management Process*, the measure needed to monitor

| | |
|---|---|
| **Question#:** | 6 |
| **Topic:** | Interagency Security Committee |
| **Hearing:** | The Navy Yard Tragedy: Examining Physical Security for Federal Facilities |
| **Primary:** | The Honorable Thomas R. Carper |
| **Committee:** | HOMELAND SECURITY (SENATE) |

compliance. With the release of the *Risk Management Process*, the ISC has approved the creation of an ISC Compliance Working Group. The primary mission of the ISC Compliance Working Group is to utilize the Interagency Security Committee's existing authority under Executive Order 12977: *Interagency Security Committee* to develop a strategy for ensuring compliance with established standards and oversee the implementation of appropriate security measures in Federal facilities. This working group will be comprised of subject matter experts brought together to address the specific issues related to compliance.

The working group will develop a method to evaluate the existing level of compliance with published ISC standards and how they are currently being implemented; develop screening criteria to evaluate compliance with ISC standards; identify resources required to fulfill the mission of compliance; and document a comprehensive strategy for compliance.

**Question:** What resources would your organization need in order to assume this responsibility?

**Response:** At this time the ISC is funded for the appropriate level of effort through NPPD's Office of Infrastructure Protection. ISC staff relies on members to support the work of the committee, including identifying current issues and drafting standards and documents. Without the support of member agencies, the ISC would be unable to carry out its important mission.

As the ISC finalizes a strategy for compliance, any additional resources will be requested through the budget process.

**Post-Hearing Questions for the Record**
**Submitted to Caitlin A. Durkovich and L. Eric Patterson**
**From Senator Tom A. Coburn, M.D.**

**"The Navy Yard Tragedy: Examining Physical Security For Federal Facilities"**

**December 17, 2013**

| | |
|---|---|
| **Question#:** | 7 |
| **Topic:** | practices and procedures |
| **Hearing:** | The Navy Yard Tragedy: Examining Physical Security for Federal Facilities |
| **Primary:** | The Honorable Tom A. Coburn |
| **Committee:** | HOMELAND SECURITY (SENATE) |

**Question:** Please provide details of any changes in practices and procedures FPS has made in wake the Washington Navy Yard shooting. Specifically address the active shooter policy and the responsibility of the contracted security officers.

**Response:** FPS is reviewing the special circumstances training that contract security guards receive to determine how it could be enhanced to better prepare contract guards to respond to an active-shooter incident.

At this time, neither the Federal Bureau of Investigation (FBI) nor the Navy has completed their investigation of the shooting at the Department of Defense facility located at Navy Yard. Once the FBI and Navy complete their investigations and their conclusions are made public, FPS will review their findings and determine whether any FPS policies, practices, and procedures should be adjusted.

| | |
|---|---|
| **Question#:** | 8 |
| **Topic:** | active shooter training |
| **Hearing:** | The Navy Yard Tragedy: Examining Physical Security for Federal Facilities |
| **Primary:** | The Honorable Tom A. Coburn |
| **Committee:** | HOMELAND SECURITY (SENATE) |

**Question:** What was FPS' rationale for the current policy changes in the response to an active shooter? Has FPS mandated active shooter training for all contracted security officers? If so, have all of your contracted security officers received this training?

**Response:** At this time, FPS has not instituted any policy changes pertaining to active shooter incident response. On November 21, 2013, FPS issued correspondence to PSO vendors regarding PSO response to active shooter incidents. The purpose of this correspondence was to reinforce PSO knowledge of their roles and responsibilities in response to an active shooter incident.

It is important to note that the initial training FPS contract security guards receive includes guidance regarding actions security guards must take in emergency and special situations such as a building fire, natural disaster, or active shooter situation. Contract security guards are not authorized to stand post for FPS until they receive this initial training and this training is validated by the security company to FPS.

Going forward, FPS plans to integrate a more robust and comprehensive active shooter training into the National Lesson Plan for PSOs and has already engaged the National Association of Security Companies and several security companies to inform this process and help identify training requirements.

| | |
|---|---|
| **Question#:** | 9 |
| **Topic:** | standards set by ISC |
| **Hearing:** | The Navy Yard Tragedy: Examining Physical Security for Federal Facilities |
| **Primary:** | The Honorable Tom A. Coburn |
| **Committee:** | HOMELAND SECURITY (SENATE) |

**Question:** Since the Interagency Security Committee (ISC) does not monitor agencies for compliance, and compliance currently is the responsibility of each individual agency, how does FPS comply with the standards set by ISC? Can you provide an example?

**(Patterson) Response:** FPS incorporated the majority of the ISC's compendium of standards that articulate the risk management process for Federal facilities into its current Facility Security Assessments (FSA) process. Specifically, the FSA process includes the ISC's FSL Determinations, Physical Security Criteria for Federal Facilities, and the Design Basis Threat as incorporated into the MIST tool to identify and mitigate vulnerabilities. FPS also conducts a threat assessment and provides a Threat Assessment Report as part of an FSA, so stakeholders have an understanding of the threats they face from the terrorism and local criminal activity perspective.

**(Durkovich) Response:** The DHS Chief Security Officer is responsible for implementing ISC standards and ensuring compliance for the Department. One example of this is the issuance of identification badges for Department employees.

| | |
|---|---|
| **Question#:** | 10 |
| **Topic:** | contract oversight |
| **Hearing:** | The Navy Yard Tragedy: Examining Physical Security for Federal Facilities |
| **Primary:** | The Honorable Tom A. Coburn |
| **Committee:** | HOMELAND SECURITY (SENATE) |

**Question:** What is the status of FPS' comprehensive and reliable system for contract oversight as recommended by GAO? What is FPS' existing process for conducting monthly file reviews? Does it require training and certification verifications?

**Response:** FPS has taken significant actions to monitor contract performance, and is utilizing a variety of reliable mechanisms, as opposed to one single comprehensive system, to provide contract oversight. These mechanisms currently include conducting regularly scheduled contract management meetings, dedicated Contracting Officer Representative (COR) oversight, tracking and recording of performance in the Contractor Performance Assessment Reporting System (CPAR), and a host of audit and inspection programs to ensure full compliance with all contractual training and certification requirements. The utilization of these various mechanisms and tools provides a system of checks and balances that benefit contract oversight in a more comprehensive manner than any currently known single system.

FPS's acquisition division tracks the contract period of performance via continuous monitoring of performance. This includes identifying performance problems as early as possible and requiring the contractor's timely resolution of any outstanding issues or problems. These issues are often identified by the COR and discussed at the regularly scheduled contract management meetings. FPS has instituted the COR Program to have national oversight and provide direction regarding the hiring of 42 full-time personnel to perform contract administration and oversight duties for FPS's contract portfolio and an FPS-specific training program outlining the requirements to perform in the capacity of a dedicated COR. The COR training program is intensive and the first FPS COR-specific training class was held for two weeks at the Federal Law Enforcement Training Center (FLETC) in December 2013. FPS expects to fill the remaining COR positions by the end of Fiscal Year (FY) 2014.

FPS continues to take measures to improve administrative audit procedures to ensure a fully trained, certified and effective PSO force is employed for the protection of Federal facilities. As to FPS' existing process for conducting monthly reviews of PSO training and certification requirements, FPS conducts an administrative audit of 10 percent of the PSO files monthly, and a 100 percent audit is immediately triggered if significant deficiencies are discovered during this process. These administrative audit procedures examine a number of factor to include training, certification and qualification records for PSOs, security fitness determination results, prior performance issues (if any), and applicable state and local licensing permits required for performance of duties. FPS has

| | |
|---|---|
| **Question#:** | 10 |
| **Topic:** | contract oversight |
| **Hearing:** | The Navy Yard Tragedy: Examining Physical Security for Federal Facilities |
| **Primary:** | The Honorable Tom A. Coburn |
| **Committee:** | HOMELAND SECURITY (SENATE) |

recently undertaken a comprehensive review of the current administrative audit procedures and found some variations when implementing the National Audit Checklist. These variations were primarily due to performance requirements in older contracts as compared to the newer contracts that generally contain more stringent training and certification requirements that have evolved as FPS continues to implement quality improvement processes.

Finally, FPS is reviewing various automated processes previously recommended by GAO that could provide FPS with electronic PSO file review capability that would supplement the current audit process. FPS is currently partnering with S&T to develop a prototype Post Tracking System that will be capable of capable of authenticating PSOs, tracking PSO time on position, and tracking PSO training and certification in real time. FPS will continue to explore these processes and adopt them to the extent they are operationally beneficial and achievable from a fiscal standpoint. It is important to note that like most other Government agencies, FPS faces challenges making investments in automating and improving its processes challenging given the current budget environment.

| | |
|---|---|
| **Question#:** | 11 |
| **Topic:** | FPS standards |
| **Hearing:** | The Navy Yard Tragedy: Examining Physical Security for Federal Facilities |
| **Primary:** | The Honorable Tom A. Coburn |
| **Committee:** | HOMELAND SECURITY (SENATE) |

**Question:** How many contracted security officers currently assigned to GSA facilities have not been trained to required FPS standards? Was initial screener training provided? What is being done to correct any discrepancy?

**Response:** FPS continues to work with private sector vendors to identify those personnel who require training in order to meet current FPS contract security guard requirements. Under all current contracts, screener training is required as part of the initial training a contract guard must complete prior to standing post. Private sector vendors are not authorized, by contract, to man a guard post with a security guard who has not been properly trained.

Please note that in 2013, FPS instituted a standardized and improved screener training plan. All security guards new to FPS contracts are receiving this training prior to entering on duty and legacy PSOs will receive the updated training during their required refresher training.

| | |
|---|---|
| **Question#:** | 12 |
| **Topic:** | actions |
| **Hearing:** | The Navy Yard Tragedy: Examining Physical Security for Federal Facilities |
| **Primary:** | The Honorable Tom A. Coburn |
| **Committee:** | HOMELAND SECURITY (SENATE) |

**Question:** What actions were taken by FPS in response to GAO reports that contracted security officers were not properly trained? What procedures or policies are in place to ensure a similar incident cannot happen again?

**Response:** To ensure the security of FPS protected facilities and in response to GAO reports that contracted security officers were not properly trained, FPS actively 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 in 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 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 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 type/level and technological advancements.

| | |
|---|---|
| **Question#:** | 13 |
| **Topic:** | risk assessments |
| **Hearing:** | The Navy Yard Tragedy: Examining Physical Security for Federal Facilities |
| **Primary:** | The Honorable Tom A. Coburn |
| **Committee:** | HOMELAND SECURITY (SENATE) |

**Question:** FPS is currently responsible for conducting risk assessments on over 9200 GSA facilities, but according to a 2012 GAO report, approximately 5,000 required facility assessments are currently backlogged? What actions will you take to address this deficiency?

**Response:** To efficiently address the backlog referenced in FY 2013, FPS scheduled FSAs for buildings with a high Facility Security Level (FSL). FPS completed over 1,818 FSAs in FY2013, prioritizing those with an FPS of Level 3, 4, and 5, and expects the FSAs for all high FSL-Level facilities to have been assessed by the end of FY 2014.

The total number of facilities scheduled for FY2014 and the subsequent years achieves a redistribution of scheduled FSAs to ensure compliance with the ISC scheduling standard. This redistribution initiative will establish and sustain a realistic workload distribution that will achieve full compliance with the scheduling standard and, by the end of FY2014, provide consistent FSA services to all high risk facilities in the portfolio.

| | |
|---|---|
| **Question#:** | 14 |
| **Topic:** | MIST |
| **Hearing:** | The Navy Yard Tragedy: Examining Physical Security for Federal Facilities |
| **Primary:** | The Honorable Tom A. Coburn |
| **Committee:** | HOMELAND SECURITY (SENATE) |

**Question:** Does the Modified Infrastructure Survey Tool (MIST) risk assessment tool align with current ISC standards? If "consequence" is not utilized as a variable, how can Risk be accurately accessed? How does this tool align with DHS' Approach to Risk Analysis?

**Response:** In conducting Facility Security Assessments FSAs, FPS Inspectors utilize the Modified Infrastructure Survey Tool (MIST) to document the existing protective posture at a facility and compare how a facility is, or is not, meeting the baseline level of protection for its Facility Security Level (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.

FPS designed its FSA process to meet the requirements of the ISC's (Risk Management Process (RMP). However, FPS is continuing to explore the inclusion of consequences into the process. Quantifying all applicable categories of consequence for Federal facilities and incorporating that into an algorithm in an assessment tool is not currently feasible as there is not an existing body of work to facilitate such development.

The FSA process is generally reflective of the Department's approach to risk analysis and management as a process, as outlined in several doctrinal references, including the DHS published "Risk Management Fundamentals."

FPS continues to work with the ISC to explore consequence and impacts in the context of Federal facilities and missions. FPS is also working with the Department's Science and Technology Directorate (S&T) to continually review risk assessment methodologies and leverage additional tools as appropriate to improve assessments and recommendations.

| | |
|---|---|
| **Question#:** | 15 |
| **Topic:** | law enforcement training |
| **Hearing:** | The Navy Yard Tragedy: Examining Physical Security for Federal Facilities |
| **Primary:** | The Honorable Tom A. Coburn |
| **Committee:** | HOMELAND SECURITY (SENATE) |

**Question:** Contracted security officers each receive law enforcement training prior to working on a federal contract (according to contract required training). In addition to this required training each officer must also be certified by the state/local law enforcement authorities (in most cases once the licensing process is completed it gives officers the same powers as sworn police officers). Based on State requirements, what percentage of your contracted security officers possesses certifications that are the same as local law enforcement?

**Response:** FPS PSOs do not receive "law enforcement training" comparable to that received by FPS law enforcement personnel at the FLETC prior to working on a Federal contract. Rather, PSOs receive 64 hours of training conducted by private security guard companies and 16 hours of training provided by the FPS during their initial training. PSOs receive an additional 40 hours of refresher training in accordance with their contracts.

This training covers areas such as ethics; crime scene protection; actions to take in special situations, such as building evacuations, safety, and fire prevention; and public relations. 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.

PSOs are not sworn law enforcement officers nor do they have law enforcement authority. Rather, PSOs authorities to perform protective services are based on state-specific laws where the PSO is employed. In most instances, PSOs rely on the 'private person' laws, also known as 'citizen's arrest' laws, of a given state as well as that state's laws relating to self-defense, defense of others, and use of force to defend property.

| | |
|---|---|
| **Question#:** | 16 |
| **Topic:** | IED |
| **Hearing:** | The Navy Yard Tragedy: Examining Physical Security for Federal Facilities |
| **Primary:** | The Honorable Tom A. Coburn |
| **Committee:** | HOMELAND SECURITY (SENATE) |

**Question:** An August 2012 OIG Report highlighted an incident where an investigation was conducted after an improvised explosive device (IED) was discovered inside the Patrick V. McNamara Federal Building in Detroit, MI. The IED was not discovered for 21 days, during which time guards visually and physically inspected the bag, and screened it with an x-ray machine. What FPS personnel were disciplined? What were the lessons learned from the FPS internal investigation? Are all contracted security officers now able to detect IEDs and utilized the screening equipment?

**Response:** FPS took corrective actions on this incident. FPS also demanded that the contractor who provided guard services took effective action to correct the problems that led to this incident. Such actions included, but were not limited to, the contractor taking appropriate disciplinary action, including employment termination of some of the guards, retraining the guards, and correcting systemic problems to avoid recurrence of this type of incident. Additionally, FPS took financial deductions from the contract and reflected the incident in the Contractor Performance Assessment Reporting System (CPARS). Once the risk to occupants at the facility was mitigated, FPS initiated corrective actions and began an in-depth review of the contract guard monitoring, training, and suitability programs. With regard to government-provided training, an FPS Special Emphasis Audit of contract guard monitoring and training in Detroit yielded results that were similar to those noted in the OIG report. In response, FPS updated post orders, to include procedures on how to handle unattended and suspicious packages at a facility, and immediately provided eight hours of training on weapons detection to 85 PSOs in Detroit using the equipment utilized at the facilities.

Additionally, FPS reviewed its related training curriculum and developed a National Weapons Detection Training Program for implementation across FPS. Program managers are making final adjustments to the policy and training program before it is provided to PSOs nationwide and incorporated into future Statements of Work and post orders. FPS Headquarters also provided training to FPS Program Managers and CORs on conducting administrative audits of training and certification records to ensure standardization nationwide.

| | |
|---|---|
| **Question#:** | 17 |
| **Topic:** | FPS Inspectors |
| **Hearing:** | The Navy Yard Tragedy: Examining Physical Security for Federal Facilities |
| **Primary:** | The Honorable Tom A. Coburn |
| **Committee:** | HOMELAND SECURITY (SENATE) |

**Question:** FPS Inspectors have the responsibility of conducting threat assessments for federal facilities; managing the contract security officers assigned to GSA facilities and providing law enforcement response at federal facilities. Have you conducted an assessment of the inspector's workload to determine efficient FPS roles and responsibilities?

**Response:** FPS 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 to crimes, threats, and other law enforcement activities in support of our protection mission. Law enforcement personnel also oversee guard posts staffed by FPS-contracted PSOs, conduct covert security tests, and actively patrol to prevent criminal and terrorist activities. Finally, our law enforcement personnel conduct 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.

The FPS workforce staffing model, developed in collaboration with the DHS Federally Funded Research and Development Center Systems Engineering and Development Institute, enables FPS to baseline current workforce requirements. The model assists managers in making staffing and allocation decisions based on available mission data and activity-based work standards, as well as in prioritizing the delivery of services to current staffing and documenting performance relative to risk.

However, staffing requirements are not static and will vary depending on the threat source/level and required capabilities. Accordingly, FPS's baseline staffing model will continue to be refined and improved for use in determining functional gaps, prioritizing those gaps, and making strategic human capital decisions to close those gaps.

Finally, to further ensure efficient utilization of law enforcement personnel, in FY 2013, FPS created dedicated positions for CORs, including for the Protective Security Officer Contracts. This effort has multiple benefits including the reassignment of administrative contract management duties from FPS Inspectors allowing them to focus on the primary protective mission of FPS. Full implementation of this initiative is expected in 2014. The FPS workforce staffing model is a component supporting the Congressional reporting requirement for an FPS Strategic Human Capital Plan.

| | |
|---|---|
| **Question#:** | 18 |
| **Topic:** | hiring strategy |
| **Hearing:** | The Navy Yard Tragedy: Examining Physical Security for Federal Facilities |
| **Primary:** | The Honorable Tom A. Coburn |
| **Committee:** | HOMELAND SECURITY (SENATE) |

**Question:** What is the FPS hiring strategy? Are you hiring personnel who have experience conducting facility risk assessments as well as law enforcement? Are you hiring personnel with law enforcement experience to spend a majority of their time accomplishing a risk assessment function?

**Response:** FPS is focused on recruiting a vibrant workforce, eager to learn new and technical skills and recruits and hires qualified applicants from a variety of backgrounds and experiences that demonstrate the requisite ability to perform both law enforcement and physical security job tasks. Each job task specialty requires a variety of specific abilities that we make every effort to find and hire.

Currently, FPS is focused on recruiting for GS-5, GS-7, and GS-9 levels and training them according to FPS mission-specific requirements. FPS actively recruits individuals with law enforcement and/or physical security backgrounds, but FPS does not place special value on one skill set over the other. FPS is proud to report that 98 percent of all new FPS employees, since the beginning of FY 2012 are former Service members.

| | |
|---|---|
| **Question#:** | 19 |
| **Topic:** | standardize FPS training |
| **Hearing:** | The Navy Yard Tragedy: Examining Physical Security for Federal Facilities |
| **Primary:** | The Honorable Tom A. Coburn |
| **Committee:** | HOMELAND SECURITY (SENATE) |

**Question:** What efforts are being made to standardize FPS training for all contracted Security Officers and FPS Inspectors? Will contracted security companies be provided training and accreditation to become FPS certified trainers? How will new training standards be instituted in the existing security contracts? Will this happen immediately?

**Response:** FPS law enforcement personnel receive standardized training at the FLETC in Georgia and in the field. This extensive, rigorous, and consistent training ensures that FPS law enforcement personnel are able to effectively conduct FSAs and respond to tens of thousands of calls for service received annually by the FPS, 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.

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 capability to validate training and facilitate rapid adjustments to training to account for changes in threat source/level and technological advancements.

Beginning in FY2014, FPS will conduct a pilot that will determine the feasibility, efficiency, and effectiveness of certifying Security Company Instructors to teach Screener Training. If the pilot is successful, FPS will seek to certify security company trainers to teach PSOs the contract required training. The train the trainer pilot is scheduled to conclude within one year and FPS hopes to begin implementation soon thereafter.

| | |
|---|---|
| **Question#:** | 20 |
| **Topic:** | risk assessment tool |
| **Hearing:** | The Navy Yard Tragedy: Examining Physical Security for Federal Facilities |
| **Primary:** | The Honorable Tom A. Coburn |
| **Committee:** | HOMELAND SECURITY (SENATE) |

**Question:** GSA is developing its own risk assessment tool, because they are not currently satisfied with the timeliness of FPS risk assessment reports. Has FPS been involved with the development of GSA's risk assessment tool?

**Response:** As a result of collaboration between GSA and FPS in recent years, FPS understands that GSA has not developed, nor do they intend to develop, a risk assessment tool.

| | |
|---|---|
| **Question#:** | 21 |
| **Topic:** | tax-payer dollars |
| **Hearing:** | The Navy Yard Tragedy: Examining Physical Security for Federal Facilities |
| **Primary:** | The Honorable Tom A. Coburn |
| **Committee:** | HOMELAND SECURITY (SENATE) |

**Question:** What is FPS' rationale for spending tax-payer dollars on senior executives' leadership training that is based on the Civil War's Battle of Gettysburg? Why is this training a priority when we have contracted security officers that have not had training on combatting an active shooter or how to use screening equipment?

**Response:** FPS is tasked with the protecting life and property and an effective leadership development program would ensure that FPS supervisors and management have the leadership ethic, skills, and courage to ensure an effective operation in a dynamic threat landscape.

Leadership development programs, such as those that are connected with the Battle of Gettysburg, are widely regarded throughout the Federal Government and the private sector and are utilized by many agencies, including the Department of Defense, many components of DHS, and the Department of Justice, to effectively teach core leadership competencies. The training is tailored to the unique needs of each agency and the FPS-specific development program would utilize a variety of proven learning styles and expert facilitators to relate real-time decision making, communication, and strategic planning in battle to supervisory, leadership and management skills required within FPS. The training program is intended for all FPS employees in a supervisory position and to date, FPS has targeted GS-13 and GS-14 level supervisors.

It is not accurate to state that the contracted security officers have not had training on combatting an active shooter or how to use screening equipment. Contracted security officers have received varying levels of active shooter awareness training and the use of screening equipment depending upon the age of the contract, the available resources in each of the FPS Regions, etc. The level and amount of training is currently under review and once finalized, the intent is to standardize all such training.

| | |
|---|---|
| **Question#:** | 22 |
| **Topic:** | NPPD |
| **Hearing:** | The Navy Yard Tragedy: Examining Physical Security for Federal Facilities |
| **Primary:** | The Honorable Tom A. Coburn |
| **Committee:** | HOMELAND SECURITY (SENATE) |

**Question:** Please provide details of any changes in practices and procedures NPPD has made in wake the Washington Navy Yard shooting. Specifically address the active shooter policy and the responsibility of the contracted security officers.

**Response:** NPPD's Office of Infrastructure Protection leads the Department's efforts to strengthen public and private sector operations by securing critical infrastructure and assisting owners and operators to prepare for threats from all hazards, including such events as an active shooter.

Prior to the Navy Yard shooting, DHS developed a suite of materials developed in partnership with the private sector to include training and awareness resources (guide book; pocket guide; break room poster), an online training program, an interactive workshop, and training videos. All of these resources are designed to assist the infrastructure owner and operator better train their staff and volunteers, plan for a mass casualty shooting event, and coordinate with first responders in a more effective and efficient manner. For example, we have hosted Active Shooter Workshops and training sessions for law enforcement and the private sector to discuss lessons learned from past active shooter situations and best practices. We also have created an active shooter page on the DHS website that has become a one-stop-shop for resources for both the public and private sector – www.dhs.gov/activeshooter – resources designed for law enforcement as well as the public on how to respond to active shooter incidents.

As a part of the Administration's comprehensive efforts to reduce gun violence following the shootings at Sandy Hook Elementary, DHS, in partnership with the Departments of Justice, Education, and Health and Human Services, has taken significant steps to improve preparedness, and strengthen security at potential targets. DHS officials joined the FBI as well as state and local law enforcement officials from around the nation to solicit input regarding prevention and response efforts. This input informed the Administration's work to create model emergency planning guidance for schools, houses of worship and institutions of higher education, which were released in June 2013. Our efforts are ongoing and we are always working to incorporate new information and mitigate potential threats.

In addition, the ISC established an Active Shooter Working Group in spring 2013 to streamline existing policy on Active Shooter situations and develop a single cohesive resource for Federal agencies and departments to enhance preparedness for an active shooter incident in a Federal facility. Although previous ISC documents addressed

| | |
|---|---|
| **Question#:** | 22 |
| **Topic:** | NPPD |
| **Hearing:** | The Navy Yard Tragedy: Examining Physical Security for Federal Facilities |
| **Primary:** | The Honorable Tom A. Coburn |
| **Committee:** | HOMELAND SECURITY (SENATE) |

Active Shooter in a number of products, such as: the *Design-Basis Threat Report*, the *Violence in the Federal Workplace: A Guide for Prevention and Response*, and *Occupant Emergency Programs: An Interagency Security Committee Guide,* the ISC determined that streamlining the existing ISC policy into a single cohesive document, with greater concentration on Active Shooter to serve as a resource for Federal agencies and departments, would enhance preparedness for an active shooter incident in a Federal facility. The 18 agencies serving on the working group include:

- United States Marshal Service (Chair)
- Department of Interior
- Department of Transportation
- Federal Aviation Administration
- Department of Energy
- Internal Revenue Service
- Smithsonian
- Federal Protective Service
- General Services Administration
- U.S. Customs and Border Protection
- Department of Homeland Security
- Pentagon Force Protection Agency
- Federal Bureau of Investigation
- Alcohol, Tobacco, and Firearms
- Department of Veterans Affairs
- Federal Law Enforcement Training Center
- U.S. Coast Guard
- National Security Staff

The working group has had numerous briefs from Federal agencies on what they are doing to mitigate the active shooter threat. Since the shooting at the Navy Yard, the working group has asked agencies who responded to the Navy Yard incident to share their lessons learned. Lessons learned from the Washington Navy Yard shooting will be incorporated into the ISC guidance.

| | |
|---|---|
| **Question#:** | 23 |
| **Topic:** | workforce |
| **Hearing:** | The Navy Yard Tragedy: Examining Physical Security for Federal Facilities |
| **Primary:** | The Honorable Tom A. Coburn |
| **Committee:** | HOMELAND SECURITY (SENATE) |

**Question:** What mechanisms are in place for Federal Agencies and Private Sector companies tasked with securing federal facilities to share best practices with its workforce and other Federal Agencies?

**Response:** Within the Federal Government, there are two important mechanisms for sharing of best practices among those responsible for securing Federal facilities. They are the Interagency Security Committee (ISC), which develops and issues standards, guidelines and best practices for use by the Federal security community, and the Government Facilities Sector Government Coordinating Council under the framework of the National Infrastructure Protection Plan.

Although lessons learned and best practices are incorporated into ISC subcommittees, working groups, standards, and products, previously there was not a dedicated ISC working group which regularly collected and incorporated best practices. As a result, great work, innovative ideas, and collective lessons learned from specific events or projects were not being shared to the fullest extent possible among the membership.

In the spring of 2012, the ISC formed a working group to promote a forum of information sharing on lessons learned. The information collected and the collaboration of the members of the law enforcement/security community provides a wealth of information and front-line expertise on effective security planning, training, and operational practices for Federal facilities and personnel; and assists the ISC members to prevent, protect against, respond to, and recover from terrorist attacks, natural disasters, criminal activities, and other emergencies at their facilities.

Topics discussed by the working group include: lessons learned from recent security incidents not raised to a national level requiring law enforcement response, best practices for measuring compliance with security standards, and identification of security measures for agencies with a diverse portfolio, among others. Best practices and lessons learned that are deemed broadly applicable and relevant to share with the broader ISC membership and their respective agencies is shared through a number of venues from briefings at ISC Quarterly meetings, through newsletters, and posted to the internal ISC portal. The working group membership consists of 14 Federal agencies and departments:

- Internal Revenue Service (Chair)
- U.S. Courts
- Nuclear Regulatory Committee

| | |
|---|---|
| **Question#:** | 23 |
| **Topic:** | workforce |
| **Hearing:** | The Navy Yard Tragedy: Examining Physical Security for Federal Facilities |
| **Primary:** | The Honorable Tom A. Coburn |
| **Committee:** | HOMELAND SECURITY (SENATE) |

- Department of Energy
- Health and Human Services
- Federal Bureau of Investigation
- Department of Transportation
- Pentagon Force Protection Agency
- United States Marshal Service
- Office of Personnel Management
- Federal Protective Service
- DHS Science and Technology
- Department of the Interior
- DHS Office of the Chief Security Officer

The National Infrastructure Protection Plan lays out a framework for the partnership between government and private sector organizations. For other sectors identified in the National Infrastructure Protection Plan, there is both a Government Coordinating Council and a Sector Coordinating Council, which includes members of industry and nongovernment organizations. FPS and GSA co-chair the Government Facilities Coordinating Council, which includes federal, state, and local government representatives and which serves as a forum for identification and discussion of security issues and challenges, and sharing of best practices among members.

| | |
|---|---|
| **Question#:** | 24 |
| **Topic:** | GAO |
| **Hearing:** | The Navy Yard Tragedy: Examining Physical Security for Federal Facilities |
| **Primary:** | The Honorable Tom A. Coburn |
| **Committee:** | HOMELAND SECURITY (SENATE) |

**Question:** Was NPPD aware of the 26 GAO recommendations provided to FPS between 2010 and 2013? Where is the accountability? Why have only four of these recommendations been addressed?

**Response:** NPPD's Audit Liaison Office is aware of all GAO recommendations assigned to NPPD, including those recommendations that FPS is responsible for addressing. NPPD is actively engaged with the GAO to provide updates and resolve recommendations. NPPD Subcomponents, including FPS, are in regular contact with the GAO to ensure that each recommendation is addressed. Between January 2004 and December 2013, GAO issued 52 recommendations to FPS. By the end of calendar year 2013, 22 of those recommendations were closed by GAO and 30 are open. Of the 30 open recommendations, three are awaiting formal closure from the Department and GAO. The timelines and details for the implementation of the 30 open recommendations are included in Attachment 1.

| | |
|---|---|
| **Question#:** | 25 |
| **Topic:** | cyber security |
| **Hearing:** | The Navy Yard Tragedy: Examining Physical Security for Federal Facilities |
| **Primary:** | The Honorable Tom A. Coburn |
| **Committee:** | HOMELAND SECURITY (SENATE) |

**Question:** NPPD has been seeking greater responsibility in the area of federal and private sector cyber security? If an agency within NPPD is struggling to effectively manage federal facility security, it raises the question of what new responsibilities NPPD deserves or can handle? What is your response?

**Response:** DHS leads the national effort to secure Federal civilian networks and coordinates the overall national effort to protect critical infrastructure and enhance cybersecurity. The Department executes its cyber mission under an existing patchwork of statutory authorities, presidential directives and Executive Orders spanning multiple Administrations. While the nation's dependence on cyber infrastructure has grown exponentially since the Department's founding, the Department's statutory authorities have not kept pace with evolving technologies and reliance on cyberspace by Federal agencies and critical infrastructure. To enable DHS and other agencies to more effectively and efficiently carry out their existing responsibilities, DHS is seeking statutory clarity of its responsibilities of supporting Federal and private sector cyber security.

NPPD has a leading role in the Department's cyber mission and has made great strides in maturing and enhancing its capabilities. The National Cybersecurity and Communications Integration Center (NCCIC) is a 24x7 incident response and management center with a proven track record of providing timely technical assistance to Federal government agencies and the private sector, including vulnerability assessments, incident response, mitigation support and cybersecurity information. In FY 2013 alone the NCCIC issued over 7,500 actionable cybersecurity alerts and products to the Federal government and private sector critical infrastructure partners, conducted dozens of assessments across critical infrastructure sectors, and deployed the Cyber Security Evaluation Tool to over 1800 critical infrastructure owners and operators to assist in performing their own cybersecurity self-assessments.

DHS has also made significant progress in expanding information sharing activities with the private sector. In 2011, DHS launched the Cyber Information Sharing and Collaboration Program (CISCP), which is specifically designed to elevate the cyber awareness of all critical infrastructure sectors through close and timely cyber threat information sharing and direct analytical exchange. Hundreds of products and thousands of indicators have been shared through CISCP already. Another avenue for information sharing is the newly operational Enhanced Cybersecurity Service (ECS) program. This effort provides another layer of protection to critical infrastructure entities by allowing

| | |
|---|---|
| **Question#:** | 25 |
| **Topic:** | cyber security |
| **Hearing:** | The Navy Yard Tragedy: Examining Physical Security for Federal Facilities |
| **Primary:** | The Honorable Tom A. Coburn |
| **Committee:** | HOMELAND SECURITY (SENATE) |

commercial service providers to utilize sensitive government cyber threat information for intrusion prevention services. The Department has also worked to provide the private sector with tools to increase sharing with other private sector partners through the development of standardized indicator sharing tools such as STIX and TAXI. These tools provide a standardized format and protocol for transferring malware indicators in a machine readable format so that partners with different systems can utilize one common language.

| | |
|---|---|
| **Question#:** | 26 |
| **Topic:** | responses and actions |
| **Hearing:** | The Navy Yard Tragedy: Examining Physical Security for Federal Facilities |
| **Primary:** | The Honorable Tom A. Coburn |
| **Committee:** | HOMELAND SECURITY (SENATE) |

**Question:** Will you please provide the date FPS submitted all responses and actions regarding the 22 previously unresolved recommendations from GAO between 2010 and 2013? Why did it take so long for FPS to respond? Did NPPD provide any pressure on FPS to implement these recommendations that are critical to the improvement of FPS and enhance the security of over 9,200 federal facilities?

**Response:** NPPD is committed to addressing all GAO recommendations and closing them in a timely and efficient manner. The NPPD Audit Liaison Office is responsible for ensuring that all GAO recommendations are addressed by the responsible program office. When a GAO recommendation pertaining to FPS is issued, NPPD Audit Liaison works with FPS to address recommendations from the Final Report and describes specific, relevant progress made to address, and possibly close, each recommendation. FPS evaluates the best approach for comprehensively addressing each recommendation, which means that some recommendations may take more time to complete than others. Closure also often depends on the complexity of the recommendation, other parties (e.g. other departments) that may be involved, and available resources.

Attachment 1 provides information pertaining to the submission of responses and actions regarding the 30 GAO recommendations open at the end of 2013.

**Post-Hearing Questions for the Record**
**Submitted to Caitlin A. Durkovich and L. Eric Patterson**
**From Senator Jon Tester**

**"The Navy Yard Tragedy: Examining Physical Security For Federal Facilities"**

**December 17, 2013**

| | |
|---|---|
| **Question#:** | 27 |
| **Topic:** | ratio |
| **Hearing:** | The Navy Yard Tragedy: Examining Physical Security for Federal Facilities |
| **Primary:** | The Honorable Jon Tester |
| **Committee:** | HOMELAND SECURITY (SENATE) |

**Question:** During questioning, Senator Coburn pointed to the relatively low ratio of one FPS law enforcement officer to every twenty-two contract PSOs. Designing and maintaining a database to report just 13,000 individuals should not take years to implement, yet the GAO has reported insufficient documentation and record keeping by FPS since 2010. Why has the establishment of a system taken so long to implement? What delays have you encountered? Have you consulted with the National Association of Security Companies and other groups? When questioned, Stephen Amitay of the National Association of Security Companies, insisted that their contractors already have the systems required to maintain records. In your estimation, would it not be a good idea to utilize the faculties these contractors already have in place to track and maintain the thousands of daily PSO records?

**Response:** To address the above-referenced pending GAO recommendations and enhance FPS's PSO oversight capability, FPS is currently working towards the development of a PSO Post Tracking System. To date, FPS has appointed a program manager, additional acquisition professionals, and initiated the development of the appropriate acquisition documents to include a Mission Needs Statement, and Capability Development Plan.

FPS is currently partnering with the DHS Science and Technology Directorate (S&T) to develop a prototype Post Tracking System that will be capable of tracking PSO time and attendance as well as training and certifications. Additionally, FPS will issue a request for information (RFI) to the vendor community to solicit potential existing capabilities that FPS could leverage in the delivery of a Post Tracking System. The RFI will include FPS requirements and will identify that FPS seeks to leverage the data already available through the security vendors and not duplicate those technologies but rather allow for consolidated Federal audit and oversight capabilities as well as the additional operational capabilities being sought.

| | |
|---|---|
| **Question#:** | 27 |
| **Topic:** | ratio |
| **Hearing:** | The Navy Yard Tragedy: Examining Physical Security for Federal Facilities |
| **Primary:** | The Honorable Jon Tester |
| **Committee:** | HOMELAND SECURITY (SENATE) |

FPS values the significant contributions that the PSOs and their companies make to protecting Federal facilities and the people in them and intends to work with these vendors as we develop and deploy the Post Tracking System.

| | |
|---|---|
| **Question#:** | 28 |
| **Topic:** | human capital planning |
| **Hearing:** | The Navy Yard Tragedy: Examining Physical Security for Federal Facilities |
| **Primary:** | The Honorable Jon Tester |
| **Committee:** | HOMELAND SECURITY (SENATE) |

**Question:** In your testimony, you stated that, "in FY 2013, the FPS has submitted documentation to the GAO for closure and consideration pertaining to 13 GAO recommendations including FPS strategies to enhance its human capital planning and improve tenant communication." Of these, you stated, "six were successfully closed as implemented and seven are pending GAO's internal review for closure." Could you please disclose which of those 13 GAO recommendations have been "successfully closed as implemented" and which are still pending GAO's internal review for closure? Furthermore, during his testimony, Mark Goldstein of the GAO insisted that only four of those GAO suggestions had been successfully implemented by the FPS. Can you please explain this discrepancy?

**Response:** FPS began 2013 with 33 open recommendations. Three new recommendations were added and six others were closed, leaving 30 open recommendations at the end of 2013. The seven recommendations submitted for closure in 2013 and the six recommendations closed in 2013 are listed in Attachment 2.

| | |
|---|---|
| **Question#:** | 29 |
| **Topic:** | MIST framework |
| **Hearing:** | The Navy Yard Tragedy: Examining Physical Security for Federal Facilities |
| **Primary:** | The Honorable Jon Tester |
| **Committee:** | HOMELAND SECURITY (SENATE) |

**Question:** GAO has complained that FPS has no real "risk assessment" system, but Director Patterson, you mentioned MIST to respond to this line of inquiry before this committee. MIST, however, does not contain an assessment of "consequences", a metric that the Interagency Security Committee recommends that every agency consider when assessing risk. It sounds to me that if a metric such as "consequences" is not easily placed into the MIST framework that it is ignored. Is it possible for consequences to be measured separately from the MIST framework? If it is difficult to consider consequences using algorithms, why do you not consider them in another way? Has FPS looked into what other agencies have done to consider consequences in their own risk assessments?

**Response:** In conducting FSAs, FPS Inspectors utilize MIST to document the existing protective posture at a facility and compare 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.

FPS designed its FSA process to meet the requirements of the ISC RMP. However, FPS is continuing to explore the inclusion of consequences into the process. Quantifying applicable categories of consequence to Federal facilities and incorporating them into an algorithm in an assessment tool is not currently feasible as there is not an existing body of work to facilitate such development.

FPS continues to work with the ISC to explore consequence and impacts in the context of Federal facilities and missions. FPS is also working with the DHS Science and Technology Directorate (S&T) to continually review risk assessment methodologies and leverage additional tools as appropriate to improve assessments and recommendations.

| | |
|---|---|
| **Question#:** | 30 |
| **Topic:** | deputizing PSOs |
| **Hearing:** | The Navy Yard Tragedy: Examining Physical Security for Federal Facilities |
| **Primary:** | The Honorable Jon Tester |
| **Committee:** | HOMELAND SECURITY (SENATE) |

**Question:** During questioning, you suggested deputizing certain PSOs in order to fulfill the shortfall of FPS inspectors at federal buildings. You expressed concern that the cost would be prohibitively expensive. What associated costs would be involved in deputizing PSOs? Has the FPS concluded a study to demonstrate how costly this process of deputizing PSOs would be? Would this be a more expensive option than hiring more FPS inspectors?

**Response:** Although I raised this concept in theory, FPS PSOs do not have law enforcement authority and FPS does not have the statutory authority to deputize PSOs as law enforcement officers. Further, FPS PSOs and FPS law enforcement personnel have different, but complementary roles and responsibilities.

FPS has not conducted training or comparative cost studies. However, it stands to reason that the costs of deputizing FPS PSOs would be prohibitively expensive (especially in this current fiscal climate) because FPS PSOs would be required to receive law enforcement, FSA, and investigative follow-up training comparable to that received by FPS law enforcement personnel at the FLETC.

Additionally, since security companies would demand a higher hourly contract rate for a Federal law enforcement officer-trained PSO, FPS contracting costs for our client agencies would rise considerably.

Accordingly, FPS PSOs are not currently authorized, trained, equipped, or compensated to assume FPS law enforcement personnel duties at Federal facilities.

| | |
|---|---|
| **Question#:** | 31 |
| **Topic:** | ISC's mission |
| **Hearing:** | The Navy Yard Tragedy: Examining Physical Security for Federal Facilities |
| **Primary:** | The Honorable Jon Tester |
| **Committee:** | HOMELAND SECURITY (SENATE) |

**Question:** According to your testimony, the ISC's mission 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." This committee in particular is very concerned about the protection of the employees working within these federal buildings and the public that visits them. A large part of keeping those people safe is ensuring that the agencies charged with protecting them are doing it the right way. Keeping these protective federal agencies accountable is a significant component addressed by the ISC's recommendations, yet these recommendations are not binding. What tools would allow ISC to compel agencies to follow its guidelines and recommendations? Why make recommendations to the different agencies if they are not being followed?

**Response:** As stated in E.O. 12977 Section 6(b) *each executive agency and department shall cooperate and comply with the policies and recommendations of the Committee issued pursuant to this order, except where the Director of Central Intelligence determines that compliance would jeopardize intelligence sources and methods.* Although the ISC develops a number of resource documents for Federal agencies and departments such as guidelines and best practices, the ISC also develops standards which are binding per Executive Order 12977. ISC guidelines and recommendations are an additional tool developed by the membership and are being followed by numerous agencies. As cited in GAO Report, 13-222, according to survey responses from 32 agencies, the ISC standards are the second most used source in developing and updating Federal agencies' physical security programs. This is second only to institutional knowledge or subject matter expertise in physical security that an agency's security staff has developed through their professional experience.

A large part of this is the result of user buy-in into the development process. The standards are created with extensive collaboration from the 53 ISC member agencies and go through a comment and voting period to allow agencies to ensure the standards, guidelines, and best practices are accurate as well as viable in practice. All standards are approved based on majority consensus.

| | |
|---|---|
| **Question#:** | 32 |
| **Topic:** | consequences |
| **Hearing:** | The Navy Yard Tragedy: Examining Physical Security for Federal Facilities |
| **Primary:** | The Honorable Jon Tester |
| **Committee:** | HOMELAND SECURITY (SENATE) |

**Question:** During questioning, Director Patterson indicated that there is no easy way to quantify the meaning of "consequences". Do you feel this is true? Do consequences need to be quantified, or can they be done using another metric? What recommendations do you have for Director Patterson to simplify this process?

**Response:** ISC standards do not require a specific metric for evaluating consequence (factors that characterize the value or criticality of the facility). It does, however, provide a method to incorporate consequence into the risk management process. Consequence does need to be considered in order to fully understand the risk and it should be noted FPS is not ignoring consequences; consequence and potential impacts are considered as part of an FSL calculation. Consequence can be quantified based on identified assets that need to be protected. For example, the number of people affected by an undesirable event, the replacement cost of assets, or the loss of specific critical functions. However, the ISC recognizes that the criteria provided in the RMP cannot capture all of the circumstances that could be encountered by an agency. Thus, the Standard includes the use of intangibles to allow the assessor to consider other factors unique to the department/agency needs or to the facility (i.e. child-care center).

In addition, although the requirement for assessment-specific judgment has been reduced to the extent possible, it may still be necessary. The ISC standards provide a baseline framework for which security professionals can make an informed decision based on the same rationale used in the development of this process.

**Question:** Director Patterson also said that the MIST tool used by FPS does not assess consequences. Why does FPS have the option of ignoring an important ISC metric in their own risk assessments? Moreover, do you feel that the consequences of the Navy Yard facility were correctly understood prior to the tragic events that transpired?

**Durkovich Response:** ISC standards require all non-military Federal agencies and departments to incorporate consequence in their risk assessments as does FPS. FPS continues to work with the ISC to explore consequence and impacts in the context of Federal facilities and missions. The Navy Yard is a military installation and is not subject to ISC standards. I do not have knowledge of the risk assessments, to include consequence factors that have been conducted at the Navy Yard; therefore, I am not in a position to provide an informed response.

Attachment 1 – Open GAO Recommendations as of December 31, 2013

| Report # | GAO FINAL Rpt. Issued | Report Title | # | Recommendation | FPS Response | Estimated Completion Date |
|---|---|---|---|---|---|---|
| GAO-10-142 | Oct-09 | Homeland Security: Greater Attention to Key Practices Would Improve the Federal Protective Service's Approach to Facility Protection | 3 | Reach consensus with GSA on what information contained in the Building Security Assessment [now called Facility Security Assessment (FSA) is needed for GSA to fulfill its responsibilities related to the protection of Federal buildings and occupants, and accordingly, establish internal controls to ensure that shared information is adequately safeguarded; guidance for employees to use in deciding what information to protect with Sensitive But Unclassified (SBU) designations; provisions for training on making designations, controlling, and sharing such information with GSA and other entities; and a review process to evaluate how well this information sharing process is working, with results reported to the Secretary regularly on a mutually agreed-to schedule. | **Concur: (Status OPEN)**<br><br>The MOA between FPS and GSA is still being held in abeyance until GSA finalizes a reorganization that will likely change the GSA signatory office | 3rd QTR 2015 |
| GAO-10-341 | Apr-10 | Homeland Security: Federal Protective Service's Contract Guard Program Requires More Oversight and Reassessment of Use of Contract Guards | 1 | Given the long-standing and unresolved issues related to FPS's contract guard program and challenges in protecting Federal facilities, employees, and the public who use these facilities, the Secretary of Homeland Security should direct the Under Secretary of National Protection and Programs Directorate (NPPD) and the Director of FPS to identify other approaches and options that would be most beneficial and financially feasible for protecting Federal facilities. | **Concur: (Status OPEN)**<br><br>FPS increased its interaction with the research and development community, through the DHS Science and Technology Directorate to better define requirements for the next generation of security technology. FPS is simultaneously testing new developments in countermeasures to assess their maximum effectiveness as part of the integrated set of countermeasures. | 4th QTR 2014 |
| GAO-10-341 | Apr-10 | Homeland Security: Federal Protective Service's Contract Guard Program Requires More Oversight and Reassessment of Use of Contract Guards | 2 | Rigorously and consistently monitor guard contractors' and guards' performance and step up enforcement against contractors that are not complying with the terms of the contract. | **Concur: (Status OPEN)**<br><br>FPS is increasing its minimum requirements for post inspection and administrative audits of individual Protective Security Officer (PSO) files from 10 percent annually to 10 percent monthly. FPS has also (1) developed and implemented a Covert Testing Program; (2) revised policies to increase the number, frequency and scope of guard post, administrative, and site inspections; (3) increased unannounced inspections by more than 100 percent during the past nine months; and (4) significantly increased its review of contract deliverables. | 4th QTR 2014 |

| Report # | GAO FINAL Rpt. Issued | Report Title | # | Recommendation | FPS Response | Estimated Completion Date |
|---|---|---|---|---|---|---|
| GAO-10-341 | Apr-10 | Homeland Security: Federal Protective Service's Contract Guard Program Requires More Oversight and Reassessment of Use of Contract Guards | 3 | Complete all contract performance evaluations in accordance with FPS and Federal Acquisition Regulations (FAR) requirements. | **Concur: (Status OPEN / GAO Internal Review in Process)**<br><br>As of December 19, 2013, FPS provided documents to the GAO intended to provide sufficient evidence for GAO to consider closing this recommendation. | 1st QTR 2014 |
| GAO-10-341 | Apr-10 | Homeland Security: Federal Protective Service's Contract Guard Program Requires More Oversight and Reassessment of Use of Contract Guards | 4 | Issue a standardized record-keeping format to ensure that contract files have required documentation. | **Non-Concur: (Status OPEN / GAO Internal Review in Process)**<br><br>As of November 26, 2013, FPS provided documents to the GAO intended to provide sufficient evidence for GAO to consider closing this recommendation. As required by the Contract Administration Improvement Plan for 2011, FPS's Acquisition Division AD submitted a final progress report to the Office of Procurement and Operations (OPO) on Jan. 4, 2012. The progress report included the achieved results in each area of weakness noted within the 2011 improvement plan. With this submission, FPS respectfully requested that GAO consider this recommendation closed / implemented. | 1st QTR 2014 |
| GAO-10-341 | Apr-10 | Homeland Security: Federal Protective Service's Contract Guard Program Requires More Oversight and Reassessment of Use of Contract Guards | 5 | Develop a mechanism to routinely monitor guards at Federal facilities outside metropolitan areas. | **Concur: (Status OPEN)**<br><br>FPS established and disseminated aggressive schedules for conducting post inspections. For Level IV facilities, the inspection frequency is a minimum of two posts (any shift) weekly, without regard to the geographic location of the facility. FPS developed and implemented the Agency Technical Representative Program. The Agency Technical Representative is an employee of a tenant agency who has the authority to act as a representative of a COTR for day-to-day monitoring of contract PSO performance. | 4th QTR 2014 |

| Report # | GAO FINAL Rpt. Issued | Report Title | # | Recommendation | FPS Response | Estimated Completion Date |
|---|---|---|---|---|---|---|
| GAO-10-341 | Apr-10 | Homeland Security: Federal Protective Service's Contract Guard Program Requires More Oversight and Reassessment of Use of Contract Guards | 6 | Provide building-specific and scenario-based training and guidance to its contract guards. | **Concur: (Status OPEN)**<br><br>FPS already uses a variety of programs and tactics to provide building-specific and scenario-based information to contract guards but is also enhancing methods of delivery and measurement of retention. Current practices include (1) Basic Training and Written Examination—instruction on a variety of scenarios that are common to contract guard functions; (2) Post Desk Books—the complete operational reference book provided for each contract security guard post; and (3) Occupant Emergency Plan Guide—a resource manual providing specific scenarios for prevention, protection, response, and recovery as they relate to emergency planning. FPS also develops and issues information and provides training on specific scenarios as new threats and needs arise. | 4th QTR 2014 |
| GAO-10-341 | Apr-10 | Homeland Security: Federal Protective Service's Contract Guard Program Requires More Oversight and Reassessment of Use of Contract Guards | 7 | Develop and implement a management tool for ensuring that reliable, comprehensive data on the contract guard program are available on a real-time basis. | **Concur: (Status OPEN)**<br><br>FPS is working in consultation with DHS's' Science and Technology Directorate(S&T) to develop a program that will function similarly to that of an access management system called the Identity Management System (IDMS). This system is designed to store, manage, and validate the binding of the individual to their suitability and training certifications for FPS's Protective Security Officer workforce. The system will be developed in compliance with HSPD-12, OMB M11-11, NIST SP-116 and The Federal Identity Credential and Access Management (FICAM). | 4th QTR 2014 |
| GAO-10-341 | Apr-10 | Homeland Security: Federal Protective Service's Contract Guard Program Requires More Oversight and Reassessment of Use of Contraet Guards | 8 | Verify the accuracy of all guard certification and training data before entering them into Risk Assessment Management Program (RAMP), and periodically test the accuracy and reliability of RAMP data to ensure that FPS management has the information needed to effectively oversee its guard program. | **Concur: (Status OPEN)**<br><br>FPS provided documentation on progress made in consultation with S&T to better refine requirements and identify systems capable of providing a more automated process for verifying and validating information prior to uploading it in our systems. This evaluation is ongoing. | 4th QTR 2014 |

| Report # | GAO FINAL Rpt. Issued | Report Title | # | Recommendation | FPS Response | Estimated Completion Date |
|---|---|---|---|---|---|---|
| GAO-11-492 | May-11 | Better Fee Design Would Improve Federal Protective Service's and other Federal Agencies' Planning and Budgeting for Security | 1 | The Secretary of Homeland Security should direct the Director of FPS to conduct regular reviews of FPS's security fees and use this information to inform its fee setting. | **Concur: (Status OPEN / GAO Internal Review in Process)**<br><br>FPS officials participated in a recommendation close out strategy meeting with GAO on July 25, 2013. During this meeting documentation was provided describing the corrective actions taken to address closure of all six recommendations in the GAO report. As a result of this meeting two of the six recommendations were closed by GAO. FPS is in the process of gathering additional data for future meetings to inform GAO of the actions taken and progress made to address closure of the remaining four recommendations associated with this audit. | 3 QTR 2014 |
| GAO-11-492 | May-11 | Better Fee Design Would Improve Federal Protective Service's and other Federal Agencies' Planning and Budgeting for Security | 3 | The Secretary of Homeland Security should direct the Director of the Federal Protective Service to make information on the estimated costs of key activities as well as the basis for these cost estimates readily available to affected parties to improve the transparency and credibility--and hence the acceptance by stakeholders--of the process for setting and using the fees. | **Concur: (Status OPEN / GAO Internal Review in Process)**<br><br>FPS officials met with GAO on July 25, 2013, to discuss FPS's actions to close out this recommendation. Specifically, at this meeting FPS presented documentation of corrective actions taken to address closure of all six recommendations included in the GAO report. As a result of this meeting two of the six recommendations were closed by GAO. FPS is in the process of gathering additional data for future meetings to inform GAO of the actions taken and progress made to address closure of the remaining four recommendations associated with this audit. | 3 QTR 2014 |

| Report # | GAO FINAL Rpt. Issued | Report Title | # | Recommendation | FPS Response | Estimated Completion Date |
|---|---|---|---|---|---|---|
| GAO-11-492 | May-11 | Better Fee Design Would Improve Federal Protective Service's and other Federal Agencies' Planning and Budgeting for Security | 4 | The Secretary of Homeland Security should direct the Director of the Federal Protective Service, in implementing our previous recommendation to evaluate the current fee structure and determine a method for incorporating facility risk, to assess and report to Congress on: (1) the current and alternative fee structures, to include the options and trade-offs discussed in this report, and if appropriate, and (2) options to fund FPS through a combination of fees and direct appropriations, to include the options and trade-offs discussed in this report. | **Concur: (Status OPEN / GAO Internal Review in Process)**<br><br>FPS officials met with GAO on July 25, 2013, to discuss FPS's actions to close out this recommendation. Specifically, at this meeting FPS presented documentation of corrective actions taken to address closure of all six recommendations included in the GAO report. As a result of this meeting two of the six recommendations were closed by GAO. FPS is in the process of gathering additional data for future meetings to inform GAO of the actions taken and progress made to address closure of the remaining four recommendations associated with this audit. | 3 QTR 2014 |
| GAO-11-492 | May-11 | Better Fee Design Would Improve Federal Protective Service's and other Federal Agencies' Planning and Budgeting for Security | 5 | The Secretary of Homeland Security should direct the Director of the Federal Protective Service to evaluate and report to Congress on options to mitigate challenges agencies face in budgeting for FPS security costs, such as: (1) an alternative account structure for FPS to increase flexibility, while retaining or improving accountability and transparency or (2) an approved process for estimating fee rates. | **Concur: (Status OPEN / GAO Internal Review in Process)**<br><br>FPS officials met with GAO on July 25, 2013, to discuss FPS's actions to close out this recommendation. Specifically, at this meeting FPS presented documentation of corrective actions taken to address closure of all six recommendations included in the GAO report. As a result of this meeting two of the six recommendations were closed by GAO. FPS is in the process of gathering additional data for future meetings to inform GAO of the actions taken and progress made to address closure of the remaining four recommendations associated with this audit. | 3 QTR 2014 |

| Report # | GAO FINAL Rpt. Issued | Report Title | # | Recommendation | FPS Response | Estimated Completion Date |
|---|---|---|---|---|---|---|
| GAO-11-554 | Jun-10 | FPS Transition from ICE to NPPD | 1 | To help ensure that DHS and Congress have reliable, accurate information on the timeframes and costs of transferring FPS from ICE to NPPD, the Secretary of Homeland Security should direct the Under Secretary for NPPD, in consultation with the Director of FPS and the Director of ICE, to improve the schedule for transferring IT services, in accordance with the transition plan, and to reflect scheduling best practices. | **Concur: (Status OPEN)**<br><br>As of August 6, 2013, the DHS Information Technology Services Office (ITSO) provided the following update to FPS. "The solicitation to create access to A LAN is being revised to reduce cost and to reduce risk to the government. The new solicitation is expected to be issued fourth quarter fiscal year 2013 with an award early in fiscal year 2014. The decision to revise the Statement of Work (SOW) was reviewed with and agreed to by FPS and National Protection & Programs Directorate (NPPD) senior leadership. Concurrently, FPS senior leadership has expressed a desire to explore the possibility of staying on the ICE platform due to the higher than anticipated transition and O&M costs." We still intend to request the cost estimate and transition schedule as part of the solicitation. However, since the revisions to the SOW agreed to by FPS and NPPD leadership will result in delays at least through FY 2013, we won't be able to provide you with the information GAO is requesting until early FY 2014 at the earliest. | 2nd QTR 2014 |
| GAO-11-554 | Jun-10 | FPS Transition from ICE to NPPD | 2 | Update the IT transition cost estimate, in accordance with cost-estimating best practices. | **Concur: (Status OPEN)**<br><br>As of August 6, 2013, the DHS Information Technology Services Office (ITSO) provided the following update to FPS. "The solicitation to create access to A LAN is being revised to reduce cost and to reduce risk to the government. The new solicitation is expected to be issued fourth quarter fiscal year 2013 with an award early in fiscal year 2014. The decision to revise the Statement of Work (SOW) was reviewed with and agreed to by FPS and National Protection & Programs Directorate (NPPD) senior leadership. Concurrently, FPS senior leadership has expressed a desire to explore the possibility of staying on the ICE platform due to the higher than anticipated transition and O&M costs." We still intend to request the cost estimate and transition schedule as part of the solicitation. However, since the revisions to the SOW agreed to by FPS and NPPD leadership will result in delays at least through FY 2013, we won't be able to provide you with the information GAO is requesting until early FY 2014 at the earliest. | 2nd QTR 2014 |

| Report # | GAO FINAL Rpt. Issued | Report Title | # | Recommendation | FPS Response | Estimated Completion Date |
|---|---|---|---|---|---|---|
| GAO-11-705R | Jul-11 | Actions Needed to Resolve Delays and Inadequate Oversight Issues with FPS' Risk Assessment and Management Program | 1 | Given the challenges FPS faced thus far with developing RAMP, technological changes that may have occurred in the last 4 years, and to help guide and ensure the successful development and implementation of any risk assessment and contract guard management system, the Secretary of Homeland Security should direct the Under Secretary of NPPD and the Director of FPS to evaluate whether it is cost-beneficial to finish developing RAMP or if other alternatives for completing FSAs and managing security guards would be more appropriate. | **Concur: (Status: RESOLVED OPEN / DHS Pending GAO formal Closure Confirmation)**<br><br>On July 1, 2013, FPS provided supporting documentation to GAO for closure consideration. Subsequently, as of November 21, 2013, GAO completed their review and sent notification to FPS that recommendations 1, 2 and 4 would be updated in their system as closed / implemented; however, per internal Departmental requirements, the recommendations are considered "Open" until the Department officially receives from the GAO a monthly listing of recommendations it has officially closed. To date, FPS and the Department are waiting for this list from the GAO, which is sent to the Department monthly. | 2nd QTR 2014 |
| GAO-11-705R | Jul-11 | Actions Needed to Resolve Delays and Inadequate Oversight Issues with FPS' Risk Assessment and Management Program | 2 | Given the challenges FPS faced thus far with developing RAMP, technological changes that may have occurred in the last 4 years, and to help guide and ensure the successful development and implementation of any risk assessment and contract guard management system, the Secretary of Homeland Security should direct the Under Secretary of NPPD and the Director of FPS to increase the use of project management best practices by managing requirements and conducting user acceptance testing for any future RAMP development efforts. | **Concur: (Status: RESOLVED OPEN / DHS Pending GAO formal Closure Confirmation)**<br><br>On July 1, 2013, FPS provided supporting documentation to GAO for closure consideration. Subsequently, as of November 21, 2013, GAO completed their review and sent notification to FPS that recommendations 1, 2 and 4 would be updated in their system as closed / implemented, however, per internal Departmental requirements, the recommendations are considered "Open" until the Department officially receives from the GAO a monthly listing of recommendations it has officially closed. To date, FPS and the Department are waiting for this list from the GAO, which is sent to the Department monthly. | 2nd QTR 2014 |

| Report # | GAO FINAL Rpt. Issued | Report Title | # | Recommendation | FPS Response | Estimated Completion Date |
|---|---|---|---|---|---|---|
| GAO-11-705R | Jul-11 | Actions Needed to Resolve Delays and Inadequate Oversight Issues with FPS' Risk Assessment and Management Program | 3 | Given the challenges FPS faced thus far with developing RAMP, technological changes that may have occurred in the last 4 years, and to help guide and ensure the successful development and implementation of any risk assessment and contract guard management system, the Secretary of Homeland Security should direct the Under Secretary of NPPD and the Director of FPS to establish a process for verifying the accuracy of Federal facility and guard training and certification data before entering them into RAMP. | **Concur: (Status OPEN / Closure Documentation submitted / Unresolved)**<br><br>PSO services will utilize an Excel file, called the Master PSO Certification File, to maintain and update PSO certification data. This certification file will be provided to and used by the Contracting Officers Technical Representatives as a certification tool to cross reference/validate information contained in vendor files with data provided during monthly administrative audit reviews. During the administrative audits, the data provided by the vendors in the Master PSO Certification File will be verified for accuracy. Once audits are completed, the FPS regions will send administrative audit data to FPS HQ for inclusion in the administrative audit database. With all of the administrative audit data in one centrally managed administrative audit database, FPS HQ will have visibility and easy access to PSO certification data. As the data is collected over time, FPS will be able to identify trends and target specific problem areas with PSO certifications. PSO training and certification data will be tracked and reported on a monthly basis. This new process will be in place until MIST is implemented and new processes for the tracking of PSO Program data are put in place. | 4th QTR 2015 |
| GAO-11-705R | Jul-11 | Actions Needed to Resolve Delays and Inadequate Oversight Issues with FPS' Risk Assessment and Management Program | 4 | Given the challenges FPS faced thus far with developing RAMP, technological changes that may have occurred in the last 4 years, and to help guide and ensure the successful development and implementation of any risk assessment and contract guard management system, the Secretary of Homeland Security should direct the Under Secretary of NPPD and the Director of FPS to develop interim solutions for completing FSAs and guard inspections while addressing RAMP's challenges. | **Concur: (Status: RESOLVED OPEN / DHS Pending GAO formal Closure Confirmation)**<br><br>On July 1, 2013, FPS provided supporting documentatioo to GAO for closure consideration. Subsequently, as of November 21, 2013, GAO completed their review and sent notification to FPS that recommendations 1, 2 and 4 would be updated in their system as closed / implemented, however, per internal Departmental requirements, the recommendations are considered "Open" until the Department officially receives from the GAO a monthly listing of recommendations it has officially closed. To date, FPS and the Department are waiting for this list from the GAO, which is sent to the Department monthly. | 2nd QTR 2014 |

| Report # | GAO FINAL Rpt. Issued | Report Title | # | Recommendation | FPS Response | Estimated Completion Date |
|---|---|---|---|---|---|---|
| GAO-11-857 | Oct-11 | Facility Protection Issues at Federal Courthouses | 1 | Instruct the Director of FPS and the Director of the Marshals Service, respectively, to jointly lead an effort, in direct consultation with other Federal stakeholders, to update the MOA on courthouse security to address the challenges discussed in the draft report. | **Concur: (Status OPEN)**<br><br>The FPS liaison to the U.S. Marshall Service (USMS) and FPS Office of General Counsel (OGC) have participated in a series of Working Group Meetings inclusive of all other parties to this MOU to further determine roles and responsibilities as it relates to the agreement. The purposes of this meeting were to review the current MOU/MAO, refine roles and responsibilities, and discuss the parameters of USMS pilot program and to propose operational amendments to the MOU. | 3rd QTR 2015 |
| GAO-11-857 | Oct-11 | Facility Protection Issues at Federal Courthouses | 2 | To the extent that steps are taken to expand the perimeter pilot project, instruct the Director of FPS, and the Director of the Marshals Service, respectively, to work collaboratively, in direct consultation with other stakeholders including the judiciary and GSA, to further assess costs and benefits, in terms of enhanced security, of expanding the pilot project to other primary courthouses, and assess all stakeholders' views about the pilot program. | **Concur: (Status OPEN)**<br><br>The FPS liaison to the U.S. Marshall Service (USMS)and FPS Office of General Counsel (OGC) have participated in a series of Working Group Meetings inclusive of all other parties to this MOU to further determine roles and responsibilities as it relates to the agreement. The purposes of this meeting were to review the current MOU/MAO, refine roles and responsibilities and discuss the parameters of USMS pilot program and to propose operational amendments to the MOU. | 3rd QTR 2015 |

| Report # | GAO FINAL Rpt. Issued | Report Title | # | Recommendation | FPS Response | Estimated Completion Date |
|---|---|---|---|---|---|---|
| GAO-12-739 | Apr-12 | Federal Protective Service: Actions needed to Access Risk and Better Manage Contract Guards at Federal Facilities. | 1 | Incorporate NIPP's risk management framework - specifically in calculating risk to include threat, vulnerability, and consequence information - in any permanent risk assessment tool. | **Concur: (Status OPEN)**<br><br>FPS is engaging with NPPD's Office of Infrastructure Protection, Interagency Security Committee (ISC) to clarify certification requirements for risk management tools based on their standards. This engagement will also provide a forum to discuss the implications of—and a return on investment for—developing a tool that incorporates all necessary components for risk-based decisions. These discussions with the ISC will inform future NPPD/FPS decisions. To date, NPPD/FPS is not aware of a risk assessment tool certified by the ISC as ISC- or NIPP-compliant. Although NPPD/FPS designed Modified Infrastructure Survey Tool (MIST) as a vulnerability assessment tool, we anticipate that through a modular development process, future efforts would incorporate other aspects of the NIPP risk management framework. However, all future actions will be subject to NPPD/FPS's availability of funds.<br><br>FPS is also considering if the calculation of a facility's security level (FSL) is an appropriate place to address consequences in the Federal facilities risk management process, as it examines mission criticality criteria and symbolism criteria, among other things. NPPD/FPS plans to make this part of its dialogue with the ISC. | 3rd QTR 2015 |
| GAO-12-739 | Apr-12 | Federal Protective Service: Actions needed to Access Risk and Better Manage Contract Guards at Federal Facilities. | 2 | Coordinate with GSA and other Federal tenant agencies to reduce any unnecessary duplication in security assessments of facilities under the custody and control of GSA. | **Concur: (Status OPEN)**<br><br>Q2FY13: FPS is engaging with the Interagency Security Committee (ISC) to clarify certification requirements for risk management tools. Q3FY13: Evaluate further action for development. NPPD/FPS is also considering if the calculation of a facility's FSL is an appropriate place to address consequences in the Federal facilities risk management process, as it examines mission criticality criteria and symbolism criteria, among other things. NPPD/FPS plans to make this part of its dialogue with the ISC | 3rd QTR 2015 |

| Report # | GAO FINAL Rpt. Issued | Report Title | # | Recommendation | FPS Response | Estimated Completion Date |
|---|---|---|---|---|---|---|
| GAO-12-739 | Apr-12 | Federal Protective Service: Actions needed to Access Risk and Better Manage Contract Guards at Federal Facilities. | 3 | Address MIST's limitations (assessing consequence, comparing risk across Federal facilities, and measuring performance) to better assess and mitigate risk at Federal facilities until a permanent system is developed and implemented. | **Concur: (Status OPEN)**<br><br>Q1FY13: FPS has identify existing government-owned assessment tools that could be used by sector partners to assess facility security. Q1FY13: FPS has assembled a team of security professionals to review and evaluate the assessment tools and make recommendations. Q2FY13: Conduct a preliminary evaluation using the assessment tools on three Government Facility Sector (GFS) buildings and provide written results. Q2FY13: Meet with the GCC working group to evaluate the preliminary evaluation written results. Q3FY13: present Government Coordinating Council (GCC) working group recommendations to the Government Facility SectorGCC | 1 QTR 2015 |
| GAO-12-739 | Apr-12 | Federal Protective Service: Actions needed to Access Risk and Better Manage Contract Guards at Federal Facilities. | 4 | Develop and implement a new comprehensive and reliable system for contract guard oversight. | **Concur: (Status OPEN)**<br><br>FPS is not currently resourced to begin the development of a technological application to enable more efficient and comprehensive oversight of a program as large in scope as the Protective Security Officer (PSO) program. Therefore, NPPD/FPS has begun collaborating with the DHS Science and Technology (S&T) Directorate to determine if technology may be available for NPPD/FPS to leverage in meeting this requirement. All actions will, however, be subject to the availability of funds given NPPD/FPS's recognized financial constraints. | 1 QTR 2015 |
| GAO-12-739 | Apr-12 | Federal Protective Service: Actions needed to Access Risk and Better Manage Contract Guards at Federal Facilities. | 5 | Verify independently that FPS's contract guards are current on all training and certification requirements. | **Concur: (Status OPEN)**<br><br>NPPD/FPS has begun collaborating with the DHS Science and Technology (S&T) Directorate to determine if technology may be available for NPPD/FPS to leverage in meeting this requirement. However, it is important to note that GAO acknowledged in their final report that, NPPD/FPS is not currently resourced to begin the development of a system or other technological applications to enable more efficient and comprehensive oversight of a program as large in scope as the Protective Security Officer (PSO) program. | 1 QTR 2015 |

| Report # | GAO FINAL Rpt. Issued | Report Title | # | Recommendation | FPS Response | Estimated Completion Date |
|---|---|---|---|---|---|---|
| GAO-12-852 | | Critical Infrastructure: DHS Needs to Refocus Its Efforts to lead the Government Facilities Sector | 1 | To enhance the effectiveness of the government facilities sector, [GAO] recommends that the Secretary direct FPS, in partnership with Infrastructure protection and [Government Coordinating] Council members, to develop and publish an action plan that identifies sector priorities and the resources required to carry out these priorities. With consideration of FPS's resource constraints, this plan should address FPS's limited progress with implementing a risk management approach and developing effective partnerships within the sector. The plan should address, at a minimum, steps needed to: develop appropriate data on critical government facilities; develop or coordinate a sector-wide risk assessment; identify effective metrics and performance data to track progress toward the sector's strategic goals; and increase the participation of and define the roles of non-Federal Council members. | **Concur: (Status OPEN)**<br><br>Independent of GAO's review, FPS has taken actions to enhance its coordination efforts as the Sector-Specific Agency for the Government Facilities Sector. These include establishing new relationships with the State, Local, Tribal, and Territorial Government Coordinating Council to ensure broader State and local participation in Sector coordination mechanisms.<br><br>FPS has worked with the Department of the Interior, the General Services Administration, and the Interagency Security Committee to conceptualize a revised structure for Government Facilities Sector management and coordination that would clarify roles and responsibilities and allow for enhanced subsector engagement among relevant partners. This revised structure will identify a working group to develop an action plan to address the following;<br><br>o Develop the appropriate tool to collect data on critical government facilities.<br>o Develop a risk assessment tool that can be used for the sector.<br>o Develop metrics and performance data required to track progress towards the sector's strategic goals.<br><br>FPS is developing a budget plan and will work with NPPD to seek a dedicated funding resource. | 3rd QTR 2015 |

| Report # | GAO FINAL Rpt. Issued | Report Title | # | Recommendation | FPS Response | Estimated Completion Date |
|---|---|---|---|---|---|---|
| GAO-13-694 | Sep-13 | Federal Protective Service: Challenges with Oversight of Contract Guard Program Still Exist and Additional Management Controls Are Needed | 1 | To improve management and Oversight of FPS's contract guard program, we recommend that the Secretary of Homeland Security direct the Under Secretary of NPPD and the Director so FPS to take immediate steps to determine which guards have not had screener or active shooter response training and provide it to them and, as part of developing a national lesson plan, decide how and how often these trainings will be provided in the future. | **Concur: (Status OPEN)**<br><br>NPPD/FPS sent a formal inquiry to all guard contract companies requesting that they provide NPPD/FPS with a list of current Protective Security Officers (PSOs) who may have not received the required government-provided screener training. NPPD/FPS is currently analyzing this list against different contract templates in effect across the Nation and against the dates recorded for PSOs trained. From this reviewed and validated list, NPPD/FPS will then employ a risk-based approach to prioritize the delivery of training for gaps identified and take action to ensure this training is completed in a timely manner.<br>NPPD/FPS will partner with industry to review all PSO lesson plans and crosswalk these with the latest PSO instruction manual and the current threat and operating environment. The result of this review will be updated, and as necessary, new lesson plans devised to meet those protection requirements. | 3rd QTR 2015 |
| GAO-13-694 | Sep-13 | Federal Protective Service: Challenges with Oversight of Contract Guard Program Still Exist and Additional Management Controls Are Needed | 2 | 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 | **Concur: (Status OPEN)**<br><br>NPPD/FPS is working in coordination with security companies through the National Association of Security Companies to develop a Train-The-Trainer PSO Training Pilot program where NPPD/FPS will train and certify contract guard company contract guard instructors to teach PSOs the NPPD/FPS Screener Training course (i.e., National Weapons Detection Training Program). The requirements and desired outcomes for the train-the-trainer concept have been identified and the associated SOW for modification pertaining to contracts selected for the pilot program participants is nearing completion. Additionally, NPPD/FPS is working on the question sets the pilot program needs to answer in order to make informed decisions on the feasibility and effectiveness of establishing a standardized instructor certification process. | 3rd QTR 2015 |

| Report # | GAO FINAL Rpt. Issued | Report Title | # | Recommendation | FPS Response | Estimated Completion Date |
|---|---|---|---|---|---|---|
| GAO-13-694 | Sep-13 | Federal Protective Service: Challenges with Oversight of Contract Guard Program Still Exist and Additional Management Controls Are Needed | 3 | Develop and implement procedures for monthly guard file reviews to ensure consistency in selecting files and verifying the results. | **Concur: (Status OPEN)**<br><br>NPPD/FPS evaluated the Administrative Audit Guide during a Special Emphasis Audit (SEA) conducted in four regions from late Oct. to late Nov. 2013. The feedback from the SEA will be used to inform NPPD/FPS senior management and provide NPPD/FPS the opportunity to construct additional requirements and standards for file contents and acceptable evidence of training and certifications, as required. NPPD/FPS will then provide the pre-audit guide and any new requirements or training standards to the CORs in the field to ensure consistency in the audit process. NPPD/FPS is currently reviewing various automated processes which could provide an electronic review capability of guard certifications and qualifications in support of the current audit process. | 3rd QTR 2015 |

Attachment 2 – GAO Recommendations Closed or Pending Closure in 2013 as of December 31, 2013

| Report # | GAO FINAL Rpt. Issued | Report Title | # | Recommendation | Status |
|---|---|---|---|---|---|
| GAO-09-749 | Jul-09 | Federal Protective Service Should Improve Human Capital Planning and Better Communicate with Tenants | 1 | To facilitate effective strategic management of its workforce, the Secretary of Homeland Security should direct the Director of FPS to improve how FPS headquarters collects data on its workforce's knowledge, skills, and abilities to help it better manage and understand current and future workforce needs. | Closed |
| GAO-09-749 | Jul-09 | Federal Protective Service Should Improve Human Capital Planning and Better Communicate with Tenants | 2 | Use these data in the development and implementation of a long-term strategic human capital plan that addresses key principles for effective strategic workforce planning, including establishing programs, policies, and practices that will enable the agency to recruit, develop, and retain a qualified workforce. | Closed |
| GAO-09-749 | Jul-09 | Federal Protective Service Should Improve Human Capital Planning and Better Communicate with Tenants | 3 | Collect and maintain an accurate and comprehensive list of all facility-designated points of contact, as well as a system for regularly updating this list. | Closed |
| GAO-09-749 | Jul-09 | Federal Protective Service Should Improve Human Capital Planning and Better Communicate with Tenants | 4 | Develop and implement a program for education and outreach to all customers to ensure they are aware of the current roles, responsibilities, and services provided by FPS. | Closed |
| GAO-10-142 | Oct-09 | Homeland Security: Greater Attention to Key Practices Would Improve the Federal Protective Service's Approach to Facility Protection | 1 | In order to move FPS toward greater use of the key practices, the Secretary should instruct the Director of FPS, in consultation, where appropriate, with other parts of DHS, GSA, and tenant agencies to provide the Secretary with regular updates, on a mutually agreed-to schedule, on the status of the Risk Assessment and Management Program (RAMP) and the National Countermeasures Program, including the implementation status of deliverables, clear timelines for completion of tasks and milestones, and plans for addressing any implementation obstacles. | Closed |

| Report # | GAO FINAL Rpt. Issued | Report Title | # | Recommendation | Status |
|---|---|---|---|---|---|
| GAO-10-142 | Oct-09 | Homeland Security: Greater Attention to Key Practices Would Improve the Federal Protective Service's Approach to Facility Protection | 2 | In conjunction with the National Countermeasures Program, to develop a methodology and guidance for assessing and comparing the cost-effectiveness of technology alternatives. | Closed |
| GAO-10-341 | Apr-10 | Homeland Security: Federal Protective Service's Contract Guard Program Requires More Oversight and Reassessment of Use of Contract Guards | 3 | Complete all contract performance evaluations in accordance with FPS and Federal Acquisition Regulations (FAR) requirements. | **Concur: (Status OPEN / GAO Internal Review in Process)**<br><br>As of December 19, 2013, FPS presented closure documentation to GAO. With this submission, FPS respectfully requested that GAO consider this recommendation closed / implemented. |
| GAO-10-341 | Apr-10 | Homeland Security: Federal Protective Service's Contract Guard Program Requires More Oversight and Reassessment of Use of Contract Guards | 4 | Issue a standardized record-keeping format to ensure that contract files have required documentation. | **Non-Concur: (Status OPEN / GAO Internal Review in Process)**<br><br>As of November 26, 2013, FPS presented closure documentation to GAO. As required by the Contract Administration Improvement Plan for 2011, FPS Acquisition Divisionsubmitted a final progress report to the Office of Procurement and Operations (OPO) on Jan. 4, 2012. The progress report included the achieved results in each area of weakness noted within the 2011 improvement plan. With this submission, FPS respectfully requested that GAO consider this recommendation closed / implemented. |

| Report # | GAO FINAL Rpt. Issued | Report Title | # | Recommendation | Status |
|---|---|---|---|---|---|
| GAO-11-492 | May-11 | Better Fee Design Would Improve Federal Protective Service's and other Federal Agencies' Planning and Budgeting for Security | 1 | The Secretary of Homeland Security should direct the Director of FPS to conduct regular reviews of FPS's security fees and use this information to inform its fee setting. | **Concur: (Status OPEN / GAO Internal Review in Process)**<br><br>FPS officials met with GAO on July 25, 2013, to discuss FPS's actions to close out this recommendation. Specifically, at this meeting FPS presented documentation of corrective actions taken to address closure of all six recommendations included in the GAO report. As a result of this meeting two of the six recommendations were closed by GAO. FPS is in the process of gathering additional data for future meetings to inform GAO of the actions taken and progress made to address closure of the remaining four recommendations associated with this audit |
| GAO-11-492 | May-11 | Better Fee Design Would Improve Federal Protective Service's and other Federal Agencies' Planning and Budgeting for Security | 3 | The Secretary of Homeland Security should direct the Director of the Federal Protective Service to make information on the estimated costs of key activities as well as the basis for these cost estimates readily available to affected parties to improve the transparency and credibility--and hence the acceptance by stakeholders--of the process for setting and using the fees. | **Concur: (Status OPEN / GAO Internal Review in Process)**<br><br>FPS officials met with GAO on July 25, 2013, to discuss FPS's actions to close out this recommendation. Specifically, at this meeting FPS presented documentation of corrective actions taken to address closure of all six recommendations included in the GAO report. As a result of this meeting two of the six recommendations were closed by GAO. FPS is in the process of gathering additional data for future meetings to inform GAO of the actions taken and progress made to address closure of the remaining four recommendations associated with this audit |

| Report # | GAO FINAL Rpt. Issued | Report Title | # | Recommendation | Status |
|---|---|---|---|---|---|
| GAO-11-492 | May-11 | Better Fee Design Would Improve Federal Protective Service's and other Federal Agencies' Planning and Budgeting for Security | 4 | The Secretary of Homeland Security should direct the Director of the Federal Protective Service, in implementing our previous recommendation to evaluate the current fee structure and determine a method for incorporating facility risk, to assess and report to Congress on: (1) the current and alternative fee structures, to include the options and trade-offs discussed in this report, and if appropriate, and (2) options to fund FPS through a combination of fees and direct appropriations, to include the options and trade-offs discussed in this report; | **Concur: (Status OPEN / GAO Internal Review in Process)**<br><br>FPS officials met with GAO on July 25, 2013, to discuss FPS's actions to close out this recommendation. Specifically, at this meeting FPS presented documentation of corrective actions taken to address closure of all six recommendations included in the GAO report. As a result of this meeting two of the six recommendations were closed by GAO. FPS is in the process of gathering additional data for future meetings to inform GAO of the actions taken and progress made to address closure of the remaining four recommendations associated with this audit |
| GAO-11-492 | May-11 | Better Fee Design Would Improve Federal Protective Service's and other Federal Agencies' Planning and Budgeting for Security | 5 | The Secretary of Homeland Security should direct the Director of the Federal Protective Service to evaluate and report to Congress on options to mitigate challenges agencies face in budgeting for FPS security costs, such as: (1) an alternative account structure for FPS to increase flexibility, while retaining or improving accountability and transparency or (2) an approved process for estimating fee rates. | **Concur: (Status OPEN / GAO Internal Review in Process)**<br><br>FPS officials met with GAO on July 25, 2013, to discuss FPS's actions to close out this recommendation. Specifically, at this meeting FPS presented documentation of corrective actions taken to address closure of all six recommendations included in the GAO report. As a result of this meeting two of the six recommendations were closed by GAO. FPS is in the process of gathering additional data for future meetings to inform GAO of the actions taken and progress made to address closure of the remaining four recommendations associated with this audit |

| Report # | GAO FINAL Rpt. Issued | Report Title | # | Recommendation | Status |
|---|---|---|---|---|---|
| GAO-11-705R | Jul-11 | Actions Needed to Resolve Delays and Inadequate Oversight Issues with FPS' Risk Assessment and Management Program | 1 | Given the challenges FPS faced thus far with developing RAMP, technological changes that may have occurred in the last 4 years, and to help guide and ensure the successful development and implementation of any risk assessment and contract guard management system, the Secretary of Homeland Security should direct the Under Secretary of NPPD and the Director of FPS to evaluate whether it is cost-beneficial to finish developing RAMP or if other alternatives for completing FSAs and managing security guards would be more appropriate. | **Concur: (Status: RESOLVED OPEN / DHS Pending GAO formal Closure Confirmation)**<br><br>On July 1, 2013, FPS provided supporting documentation to GAO for closure consideration. Subsequently, as of November 21, 2013, GAO completed their review and sent notification to FPS that recommendations 1, 2 and 4 would be updated in their system as closed / implemented; however, per internal Departmental requirements, the recommendations are considered "Open" until the Department officially receives from the GAO a monthly listing of recommendations it has officially closed. To date, FPS and the Department are waiting for this list from the GAO, which is sent to the Department monthly. |
| GAO-11-705R | Jul-11 | Actions Needed to Resolve Delays and Inadequate Oversight Issues with FPS' Risk Assessment and Management Program | 2 | Given the challenges FPS faced thus far with developing RAMP, technological changes that may have occurred in the last 4 years, and to help guide and ensure the successful development and implementation of any risk assessment and contract guard management system, the Secretary of Homeland Security should direct the Under Secretary of NPPD and the Director of FPS to increase the use of project management best practices by managing requirements and conducting user acceptance testing for any future RAMP development efforts. | **Concur: (Status: RESOLVED OPEN / DHS Pending GAO formal Closure Confirmation)**<br><br>On July 1, 2013, FPS provided supporting documentation to GAO for closure consideration. Subsequently, as of November 21, 2013, GAO completed their review and sent notification to FPS that recommendations 1, 2 and 4 would be updated in their system as closed / implemented; however, per internal Departmental requirements, the recommendations are considered "Open" until the Department officially receives from the GAO a monthly listing of recommendations it has officially closed. To date, FPS and the Department are waiting for this list from the GAO, which is sent to the Department monthly. |

| Report # | GAO FINAL Rpt. Issued | Report Title | # | Recommendation | Status |
|---|---|---|---|---|---|
| GAO-11-705R | Jul-11 | Actions Needed to Resolve Delays and Inadequate Oversight Issues with FPS' Risk Assessment and Management Program | 3 | Given the challenges FPS faced thus far with developing RAMP, technological changes that may have occurred in the last 4 years, and to help guide and ensure the successful development and implementation of any risk assessment and contract guard management system, the Secretary of Homeland Security should direct the Under Secretary of NPPD and the Director of FPS to establish a process for verifying the accuracy of federal facility and guard training and certification data before entering them into RAMP. | **Concur: (Status OPEN / Closure Documentation submitted / Unresolved)**<br><br>7.1.2013: FPS presented supporting documentation to GAO for closure consideration. Please note response below:<br><br>PSO services will utilize an Excel file, called the Master PSO Certification File, to maintain and update PSO certification data. This certification file will be provided to and used by the Contracting Officers Technical Representatives as a certification tool to cross reference/validate information contained in vendor files with data provided during monthly administrative audit reviews. During the administrative audits, the data provided by the vendors in the Master PSO Certification File will be verified for accuracy. Once audits are completed, the FPS regions will send administrative audit data to FPS HQ for inclusion in the administrative audit database. With all of the administrative audit data in one centrally managed administrative audit database, FPS HQ will have visibility and easy access to PSO certification data. As the data is collected over time, FPS will be able to identify trends and target specific problem areas with PSO certifications. PSO training and certification data will be tracked and reported on a monthly basis. This new process will be in place until MIST is implemented and new processes for the tracking of PSO Program data are put in place. |

| Report # | GAO FINAL Rpt. Issued | Report Title | # | Recommendation | Status |
|---|---|---|---|---|---|
| GAO-11-705R | Jul-11 | Actions Needed to Resolve Delays and Inadequate Oversight Issues with FPS' Risk Assessment and Management Program | 4 | Given the challenges FPS faced thus far with developing RAMP, technological changes that may have occurred in the last 4 years, and to help guide and ensure the successful development and implementation of any risk assessment and contract guard management system, the Secretary of Homeland Security should direct the Under Secretary of NPPD and the Director of FPS to develop interim solutions for completing FSAs and guard inspections while addressing RAMP's challenges. | **Concur: (Status: RESOLVED OPEN / DHS Pending GAO formal Closure Confirmation)**<br><br>On July 1, 2013, FPS provided supporting documentation to GAO for closure consideration. Subsequently, as of November 21, 2013, GAO completed their review and sent notification to FPS that recommendations 1, 2 and 4 would be updated in their system as closed / implemented; however, per internal Departmental requirements, the recommendations are considered "Open" until the Department officially receives from the GAO a monthly listing of recommendations it has officially closed. To date, FPS and the Department are waiting for this list from the GAO, which is sent to the Department monthly. |

CHARRTS No.: SHSGAC-06-001
Senate Committee on Governmental Affairs
Hearing Date: December 13, 2013
Subject: The Navy Yard Tragedy: Examining Physical Security for Federal Facilities.
Witness: Mr. Lewis
Senator: Senator Coburn
Question: #1

Practices and Procedures

Question. Please provide details of any changes in practices and procedures DOD has made in wake the Washington Navy Yard shooting. Specifically address the active shooter policy and the responsibility of the contracted security officers.

Answer. In the wake of the September 16, 2013, Washington Navy Yard shooting incident, the Secretary of Defense initiated concurrent independent and internal reviews to identify and recommend actions that address gaps or deficiencies in DoD programs, policies and procedures regarding security at DoD installations and the granting and renewing of security clearances for DoD employees and contractor personnel. The Under Secretary of Defense for Intelligence consolidated key recommendations from each of these reviews into a final report and provided it to the Secretary of Defense. If approved, these recommendations will be addressed in an implementation plan, in coordination with the DoD Components and key interagency partners, to include the Office of the Director of National Intelligence and the Office of Personnel Management.

CHARRTS No.: SHSGAC-06-002
Senate Committee on Governmental Affairs
Hearing Date: December 13, 2013
Subject: The Navy Yard Tragedy: Examining Physical Security for Federal Facilities.
Witness: Mr. Lewis
Senator: Senator Coburn
Question: #2

Practices and Procedures

Question. What mechanism is in place for FPS to share best practices with its workforce, Private Industry and other Federal Agencies?

Answer. The following reflects our understanding of the role and responsibilities of the Federal Protective Service (FPS), based upon our participation in the critical infrastructure sector partnership framework and the Interagency Security Committee (ISC). 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, effectiveness and efficiency. FPS is also on both the Active Shooter-Prevention and Response and the Presidential Policy Directive (PPD) 21 and Compliance working groups that are currently underway. FPS 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. The Department recommends contacting FPS for additional information.

CHARRTS No.: SHSGAC-06-003
Senate Committee on Governmental Affairs
Hearing Date: December 13, 2013
Subject: The Navy Yard Tragedy: Examining Physical Security for Federal Facilities.
Witness: Mr. Lewis
Senator: Senator Coburn
Question: #3

Interagency Security Committee

Question. Since the Interagency Security Committee (ISC) does not monitor agencies for compliance, and compliance currently is the responsibility of each individual agency, how does DOD comply with the standards set by ISC? Can you provide an example?

Answer. On December 7, 2012, the Deputy Secretary of Defense directed that the security standards, established by the Department of Homeland Security's Interagency Security Committee in the Risk Management Process for Federal Facilities, apply to all off-installation leased space managed by DoD and all DoD occupied spaced in buildings owned or operated by the U.S. General Services Administration. Key DoD Antiterrorism (AT) policy (DoD Instruction 2000.12) and guidance (Unified Facilities Criteria 04-010-01) were updated to codify this requirement, where compliance with the standards set by the ISC is subject to higher-headquarters AT program review.

CHARRTS No.: SHSGAC-06-004
Senate Committee on Governmental Affairs
Hearing Date: December 13, 2013
Subject: The Navy Yard Tragedy: Examining Physical Security for Federal Facilities.
Witness: Mr. Lewis
Senator: Senator Coburn
Question: #4

Federal Protective Service

Question. What mechanism is in place for FPS to share best practices with its workforce, Private Industry and other Federal Agencies?

Answer. Within the Federal government, there are two important mechanisms for sharing of best practices among those responsible for securing Federal facilities. They are the Interagency Security Committee, which develops and issues standards, guidelines and best practices for use by the Federal security community, and the Government Facilities Sector Government Coordinating Council under the National Infrastructure Protection Plan.

Federal Protective Services (FPS) and the U.S. General Services Administration (GSA) co-chair the council and it serves as a forum for identification and discussion of security issues and challenges and for sharing of best practices among members. More recently, FPS has begun to think through engaging the security industry on the formation of a Government Facilities Sector Coordinating Council to incorporate its perspective, challenges and best practices into the work of the sector.

CHARRTS No.: SHSGAC-06-005
Senate Committee on Governmental Affairs
Hearing Date: December 13, 2013
Subject: The Navy Yard Tragedy: Examining Physical Security for Federal Facilities.
Witness: Mr. Lewis
Senator: Senator Coburn
Question: #5

Contracted Security Officers

Question. What authorities do your contracted security officers have at DOD facilities? By what mechanism are those authorities granted (by the military, state or local jurisdiction, or a combination thereof)?

Answer. DoD policy for law enforcement and security guard standards and training establishes the responsibilities and authorities for military and DoD civilian law enforcement officers, as well as, contracted security guards. Additionally, DoD contracts with private-sector vendors require that the individual vendor obtain all required state and local licensing, permits, and authorities required for contracted security officers to perform security services at DoD facilities. Therefore a contracted security officer's authorities to perform security services are based largely on state-specific laws where the contract security officer is employed. In most instances, contracted security officers rely on the 'private person' laws, also known as 'citizen's arrest' laws, of a given state as well as that state's laws relating to self-defense, defense of others and use of force to defend property. Contracted security guards outside the United States must operate in compliance with host nation laws.

CHARRTS No.: SHSGAC-06-006
Senate Committee on Governmental Affairs
Hearing Date: December 13, 2013
Subject: The Navy Yard Tragedy: Examining Physical Security for Federal Facilities.
Witness: Mr. Lewis
Senator: Senator Coburn
Question: #6

Interagency Security Committee

Question. What ISC subcommittees does DOD belong to? Does this membership allow collaboration with private sector and other federal agencies to share facility security best practices? How has that benefited your security efforts?

Answer. DoD actively participates on the Interagency Security Committee (ISC) Steering Subcommittee and has representatives on a number of other ISC subcommittees and working groups, including the Design-Basis Threat, Active Shooter-Prevention and Response, Facility Security Planning, Facility Security Level, Facility Security Committee and Resource Management. Membership in these forums enable the sharing of best practices, physical security standards and cyber and terrorist threat information in our collective resolve to enhance the quality and effectiveness of physical security of Federal facilities. The Department's participation on the ISC subcommittees/working groups provides a mechanism to harmonize its facility security posture with other Federal departments/agencies.

CHARRTS No.: SHSGAC-06-007
Senate Committee on Governmental Affairs
Hearing Date: December 13, 2013
Subject: The Navy Yard Tragedy: Examining Physical Security for Federal Facilities.
Witness: Mr. Lewis
Senator: Senator Coburn
Question: #7

DoD IG Report

Question. A recent DOD Inspector General report revealed that 52 convicted felons received routine, unauthorized installation access, placing military personnel, dependents, civilians, and installations at an increased security risk. It was determined that this lapse occurred because the Navy Installations Command did not perform a comprehensive business case analysis and issued policy that prevented transparent cost accounting of Navy Commercial Access Control System. What actions have been taken to correct this security threat from happening in the future?

Answer. The Navy Installations Command completed a National Crime Information Center (NCIC) check of those persons who were previously issued a Navy Commercial Access Control System credential without the minimum NCIC check. Based upon the results of the NCIC check, those individuals who were deemed to pose an unacceptable risk were denied continuing access to DoD installations. The Department of Navy continues to work with the DoD Inspector General to resolve the recommendations contained in the report. Further, guidance was issued to DoD Components to ensure minimum NCIC checks are accomplished for visitors requiring routine, unescorted access to DoD installations. For those installations that lack NCIC query capabilities, they were requested to develop alternative arrangements with a nearby military installation or assigned defense criminal investigative organization as the Department continues to pursue an enterprise solution.

CHARRTS No.: SHSGAC-06-008
Senate Committee on Governmental Affairs
Hearing Date: December 13, 2013
Subject: The Navy Yard Tragedy: Examining Physical Security for Federal Facilities.
Witness: Mr. Lewis
Senator: Senator Coburn
Question: #8

On-site Communication

Question. One of the concern's in the aftermath of the Navy Yard shooting was on site communication. Several media sources reported "People running through the building yelling "get out," and an unclear speaker system saying take shelter, a fire alarm signaling evacuation. Chaos as you might expect." What has been done to establish clear direction and communication in the event of any future incident at a DOD facility?

Answer. DoD installation emergency management policy directs that all DoD installations develop mass warning and notification capabilities with the ability to warn all personnel within 10 minutes of incident notification. Further, Departmental guidance provides construction requirements for mass warning and notification systems in buildings. Additionally, DoD requires security personnel to be properly trained and equipped to respond to a broad array of security threats. This includes possessing the integrated capability for communications that are secure and diverse, used for command and control to aid in the prevention and response against sabotage, damage, terrorism and criminal activity. Emergency response equipment, when possible, is interoperable with equipment used by mutual aid partners in local communities. Since the Washington Navy Yard shooting incident, the Department has purchased Unity P-25 compliant radios, which are able to communicate with other federal agencies and civilian first responders. In addition, the Federal government has established a national capital region (NCR) emergency talk group to facilitate communication between local, state and federal first responders within the NCR.

CHARRTS No.: SHSGAC-06-009
Senate Committee on Governmental Affairs
Hearing Date: December 13, 2013
Subject: The Navy Yard Tragedy: Examining Physical Security for Federal Facilities.
Witness: Mr. Lewis
Senator: Senator Tester
Question: #9

Active Shooter Working Group

Question. In March 2013, the Interagency Security Committee established an Active Shooter Working Group to review agency actions. Since the tragic events at the Navy Yard, the Department of Defense has promised to release a report compiled from independent reviews and is expected to be released within the next few months. Mr. Lewis, would you mind updating us on the status of this report?

Answer. In the wake of the September 16, 2013, Washington Navy Yard shooting incident, the Secretary of Defense initiated concurrent independent and internal reviews to identify and recommend actions that address gaps or deficiencies in DoD programs, policies, and procedures regarding security at DoD installations and the granting and renewing of security clearances for DoD employees and contractor personnel. The Under Secretary of Defense for Intelligence consolidated key recommendations from each of these reviews into a final report and provided it to the Secretary of Defense. If approved, these recommendations will be addressed in an implementation plan, in coordination with the DoD Components and key interagency partners, to include the Office of the Director of National Intelligence and the Office of Personnel Management.

CHARRTS No.: SHSGAC-06-010
Senate Committee on Governmental Affairs
Hearing Date: December 13, 2013
Subject: The Navy Yard Tragedy: Examining Physical Security for Federal Facilities.
Witness: Mr. Lewis
Senator: Senator Tester
Question: #10

Contract Security Personnel

Question. According the reports from the Department of Defense, they are moving away from the practice of hiring contract security personnel to protect and defend military buildings and premises. Why was the decision made to make this transition away from contracted security personnel? Moreover, what progress is being made in the Department's attempts to transition away from contract security personnel? Do you believe that the reasons the Department of Defense is moving away from contractors would also apply to other federal agencies or buildings? Would you recommend that other agencies follow the facility and personnel security structures used by the Department of Defense?

Answer. Section 2465 of Title 10, United States Code, prohibits DoD from using contracted security guards. Section 332 of P.L. 107-314 was intended to provide temporary relief from this statute by allowing the Department to use contracted security guards due to increased security requirements at DoD installations following the terrorist events on September 11, 2001, and the subsequent demand for military police personnel to support operations in Iraq and Afghanistan. Section 332 was amended in FY 2008 (P.L. 110-181) to extend DoD's authority to use contracted security guards through FY 2012, but it also required the Department to reduce the number of contracted security guards by 10 percent per year, so that contracted security guards would make up no more than 50 percent of the number in the FY 2006 baseline.

The Department did not seek an extension of Section 332 authority. First, we were mindful of the general statutory prohibition on the use of contracted security guards, as reflected in Section 2465. Second, contract guards can only perform installation/facility access control functions; they cannot execute the full range of law enforcement duties required on an installation because some of this work is defined as inherently governmental in the Federal Activities Inventory Reform Act of 1998 (P.L. 105-270). Accordingly, DoD Components have put in place the requisite staffing plans to replace contracted security guards with military personnel and DoD civilian employees. The Department of Defense operates in an environment that is unique from most other federal agencies. Therefore we recommend other agencies utilize facility and personnel security structures that improve security tailored to their missions and operating environments while simultaneously driving long-term efficiencies.

GAO U.S. GOVERNMENT ACCOUNTABILITY OFFICE

**441 G St. N.W.**
**Washington, DC 20548**

February 5, 2014

The Honorable Thomas R. Carper
Chairman
Committee on Homeland Security and Governmental Affairs
United States Senate

Subject: *Responses to Questions for the Record: Committee on Homeland Security: December 17, 2013, Hearing on "The Navy Yard Tragedy: Examining Physical Security for Federal Facilities"*

Dear Chairman Carper:

This letter responds to your January 7, 2014, request that we address questions submitted for the record related to the hearing entitled "The Navy Yard Tragedy: Examining Physical Security for Federal Facilities," on December 17, 2013. Our answers to these questions are enclosed and are based on our previous and ongoing work.

If you have any questions or would like to discuss our responses, please contact me at (202) 512-2834 or GoldsteinM@gao.gov

Sincerely yours,

Mark L. Goldstein, Director
Physical Infrastructure Issues

Enclosure

cc: The Honorable Tom Coburn, Ranking Member
Committee on Homeland Security and Governmental Affairs

**Post-Hearing Questions for the Record**
**Submitted to Mark Goldstein**
**from Senator Tom Coburn**

**"The Navy Yard Tragedy: Examining Physical Security for Federal Facilities"**
**December 17, 2013**

**1. For many years GAO has investigated FPS, in your work over the past five years, what areas of possible duplicative efforts have you found in FPS training and/or risk assessments?**

We reported in 2012[1] that there is duplication in the federal government's approach to assessing risks at some of the approximately 9,000 federal facilities managed by GSA. Multiple federal agencies are expending additional resources to assess their own facilities although they pay FPS for similar services.

**2. What mechanisms are in place for Federal Agencies and Private Sector companies tasked with security federal facilities to share best practices with its workforce and other Federal Agencies?**

We have not conducted work in this area, but note that the Intelligence Reform and Terrorism Prevention Act of 2004 mandated the creation of an Information Sharing Environment (ISE) to facilitate the sharing of terrorism information among appropriate federal, state, local, and tribal entities and private sector entities through the use of policy guidelines and technologies.[2] The House Homeland Security Committee has asked GAO to review what efforts FPS has taken to comply with ISE, their effectiveness, and related issues.

**3. How did FPS develop a risk assessment backlog of over 5,000 reports? What failures in the risk assessment program have led to such ineptness?**

We reported in 2012[3] that the backlog was the result of FPS's inability to carry out risk assessments in a manner consistent with federal standards, as the agency had originally planned. Furthermore, we were unable to determine the extent of FPS's backlog because the data were unreliable.

**4. Do you know how far along GSA is in the development of a facility risk assessment tool? Do you believe they have the capability to accomplish this take for all of their 9,286 facilities?**

GSA has developed a risk assessment tool (referred to as RAMPART). However, we have not evaluated the tool's capabilities.

---

[1]GAO, *2012 Annual Report: Opportunities to Reduce Duplication, Overlap, and Fragmentation, Achieve Savings, and Enhance Revenue,* GAO-12-342SP (Washington, D.C.: Feb. 28, 2012).

[2] Pub. L. No. 108-458, § 1016, 118 Stat. 3638, 3664-70.

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

**5. Has GAO investigated the issue of limited jurisdiction for state and local first responders to federal facilities, to discover in what jurisdictions these conflicts might exist? If so, have the appropriate measures been put in place by FPS to ensure state and local law enforcement personnel can access the federal facility in the event of an emergency?**

We reported in 2008[4] that many FPS and local law enforcement officials in the regions we visited stated that jurisdictional authority would pose a significant barrier to gaining the assistance of local law enforcement agencies. We recommended that FPS clarify roles and responsibilities of local law enforcement agencies with regard to responding to incidents at GSA facilities. In 2012[5], we reported that FPS has a reasonable approach to state and local collaboration. For example, FPS has guidance that addresses issues such as the scope of law enforcement authorities on federal property and information sharing among jurisdictions. However, we have not evaluated the effectiveness of this guidance.

---

[4]GAO, *Homeland Security: The Federal Protective Service Faces Several Challenges That Hamper Its Ability to Protect Federal Facilities,* GAO-08-683 (Washington, D.C.: June 11, 2008).

[5]GAO, *Federal Protective Service: Better Data on Facility Jurisdictions Needed to Enhance Collaboration with State and Local Law Enforcement,* GAO-12-434 (Washington, D.C.: March 27, 2012).

**Post-Hearing Questions for the Record**
**Submitted to Mark Goldstein**
**from Senator Thomas R. Carper**

**"The Navy Yard Tragedy: Examining Physical Security for Federal Facilities"**
**December 17, 2013**

**1. At the hearing, you noted that Federal Protective Service personnel struggle to keep up with the amount and variety of work expected of them. Do you believe the Federal Protective Service should reexamine its workforce composition?**

We recommended in 2008[6] that FPS develop and implement a strategic approach to manage its staffing resources that, among other things, determines the optimum number of employees needed to accomplish its facility protection mission and take steps to develop a strategic human capital plan to better manage its workforce needs. Although FPS has addressed our recommendations, it has not finalized its human capital plan.

**2. Do you believe the Federal Protective Service might be more effective if it received a direct appropriation, and could pay for the security measures it recommended, rather than request that tenant agencies pay for those security measures?**

We reported in 2011[7] that modifying the current fee structure or funding FPS through a combination of fees and direct appropriations may address equity and cross-subsidization issues and improve transparency to customers, but without detailed activity cost information and a full fee review the relative trade-offs in any particular proposal are unclear. As such, we recommended that FPS evaluate its current and alternative funding and budget account structures to mitigate budget timing and other issues. FPS agreed but has not implemented our recommendation.

---

[6]GAO, *Homeland Security: The Federal Protective Service Faces Several Challenges That Hamper Its Ability to Protect Federal Facilities*, GAO-08-683 (Washington, D.C.: June 11, 2008).

[7]GAO, *Budget Issues: Better Fee Design Would Improve Federal Protective Service's and Federal Agencies' Planning and Budgeting for Security*, GAO-11-492 (Washington, D.C.: May 20, 2011).

Post-Hearing Questions for the Record
Submitted to Stephen Amitay
From Senator Thomas R. Carper

"The Navy Yard Tragedy: Examining Physical Security at Federal Facilities"
December 17, 2013

**1. What has the National Association of Security Companies or any of its member organizations done since the Washington Navy Yard shooting to address the active shooter threat to federal facilities?**

- NASCO and its member companies who are FPS contractors met with FPS to provide input on PSO active shooter training options that can/will be added to the currently FPS mandated training for PSO's. We will continue to work with FPS to effectively develop and roll out FPS PSO active shooter training that should be conducted by certified contractor trainers. .
- The companies have also directed their onsite supervisors and managers to review active shooter Post Orders and Standard Operating Procedures (SOPs) with PSO's.
- Some companies already provide active shooter training/orientation to their PSO's (which is outside the requirements of the FPS contracts and thus provided at the company's expense). Other companies are now adding active shooter training/orientation to outside PSO training.
- At other agencies where FPS contractors also provide security, some companies are conducting active shooter training and tabletop exercises with those agencies that also involve FPS PSO's and management staff.
- Some companies are now requiring their Supervisory and Federal Contract Management personnel to take and complete DHS/FEMA Emergency Management Institute (EMI) course IS-00907: "Active Shooter: What you can do."
- Some companies have issued ballistic vests to all their PSO's (which is not required in all FPS contracts).

**2. At the hearing, GAO noted that Federal Protective Service personnel struggle to keep up with the amount and variety of work expected of them. Do you believe the Federal Protective Service should reexamine its workforce composition?**

The FPS workforce is spread thin often doing multiple jobs from facility security assessments, to law enforcement duties, to investigations, to contracting officer representative (COR) to PSO trainer, and the result can often be that none of these tasks are done particularly well. Also, certain key positions such as COR's seem to be understaffed in comparison with other federal agencies that use contract security. FPS' primary mission is to protect federal facilities and FPS should re-focus on that mission and its personnel should have more focus on less functions. Inspectors do not need to be conducting PSO training and like at other federal agencies that use contract security, this training should be done by certified contractor trainers with FPS oversight. It is a big step in the right direction that FPS has recently stood up a dedicated cadre of Contract Officer Representatives (COR's). Also, in some areas, such as the National Capital Region, when a violent/criminal incident occurs, it is the D.C. Police who is the primary responder, not FPS. FPS could likely devote more resources to core federal facility protection (facility security assessments, working with facility security committees, conducting post inspections and working with contractors to ensure the PSO's are performing) than responding to incidents. FPS

should consider migrating toward becoming more of an 'oversight' agency and reducing their direct law enforcement and operational capability.

**3. Do you believe the Federal Protective Service might be more effective if it received a direct appropriation, and could pay for the security measures it recommended, rather than request that tenant agencies pay for those security measures?**

There are arguments that can be made for and against direct appropriations, although the stronger argument seems to be for direct appropriations. One the one hand, a direct appropriation would better ensure that security countermeasures recommended by FPS are indeed funded and put in place and it's likely that necessary changes to a building's security could be funded and implemented more quickly with direct appropriations. It is well documented that some tenant facility security committees are undereducated on security issues and/or willing to assume risk primarily because of budgetary and/or customer service concerns. On the other hand, as also documented, FPS is not performing all the tasks (such as risk assessments and regular post inspections) that it is being paid to perform, and some federal tenants are loathe to give up the purse strings, and resulting influence, over FPS. Some contractors have suggested that some FPS functions, such as facility security assessments, be directly appropriated, but the rest can be funded through the current method

**4. NASCO has suggested that there is a conflict between federal guidance and state laws, when it comes to responding to an active shooter. Guidance distributed by the Federal Protective Service appears to limit the authority of armed guards protecting federal facilities, while some state laws may require armed guards intercede in the event of an active shooter. In other states, the law may constrain a security guard from taking certain actions, such as interdicting an active shooter. How do security companies and security guards reconcile these conflicting requirements?**

NASCO has pointed out to FPS that its guidance to PSO's (the Security Guard Information Manual and Post Orders) which are part of the contract Statement of Work and/or the contract, can in some jurisdictions (such as Virginia) take away powers granted to state licensed security officers (which all PSO's must be) to act in violent situation. They also create great uncertainty as to what a PSO can do to react to an active shooter and the liability the PSO and contractor might face if a PSO leaves his post to respond to an active shooter. As a result, this has created an atmosphere where the contractor and PSO feel that unless they follow FPS guidance there could be serious repercussions. Thus, when there is a perceived difference between state law and FPS, the path likely chosen is to abide by the specific requirements and guidance provided in the contract Statement of Work (SOW). FPS can do a better job of reconciling state law related to active shooter situations/arrest authority to its guidance. In addition, without specific FPS mandated training on active shooter situations, a PSO is additionally hamstrung in being able to respond.

Post-Hearing Questions for the Record
Submitted to Stephen Amitay
From Senator Tom Coburn

"The Navy Yard Tragedy: Examining Physical Security at Federal Facilities"
December 17, 2013

**1. Please detail any significant changes in practices and procedures the members of NASCO have made in wake the Washington Navy Yard shooting. Specifically address the active shooter policy and the responsibility of the contracted security officers.**

See answer provided to Senator Carper's similar question for the record:

*What has the National Association of Security Companies or any of its member organizations done since the Washington Navy Yard shooting to address the active shooter threat to federal facilities?*

**2. What mechanisms are in place for Federal Agencies and Private Sector companies tasked with securing federal facilities to share best practices with its workforce and other Federal Agencies?**

NASCO and its members who are contractors at multiple federal agencies are providing information to FPS on best practices related to the use of contract security that are being employed by other federal agencies and governmental entities. Such topics include active shooter training, contracting, general training, firearms qualifications, etc. There is not much of a record though of FPS incorporating outside best practices and/or contractor input and there is no formal process to consider recommendations (unlike at other agencies). And often, when input is solicited, it is after a new policy or protocol has been put in place. Recently though, FPS has been reaching out more to other federal agencies and to the private sector to share best practices. NASCO believes it would be very valuable for agencies that share similar security requirements and mandates to work more closely together and to also include the private sector. More needs to be done to encourage and facilitate the sharing of best practices.

**3. Since the Interagency Security Committee (ISC) does not monitor agencies for compliance, and compliance currently is the responsibility of each individual agency, do your members use the standards set by the ISC? How have these standards enhanced your security efforts?**

FPS's training, screening, and other requirements for PSO's are almost identical to the requirements set out in the ISC 'best practice" (and soon to become a mandatory Standard) for armed security officers working at federal facilities. FPS was heavily involved in the development of that Standard, and NASCO also provided input into the Standard. The Association views the ISC work as a good baseline Standard.

**4. Do the security officers your companies provide to FPS currently possess the authorities required by state/local law enforcement to engage an active shooter? What needs to happen in order to align the authorities needed by officers and the level of response expected in the event of an active shooter emergency?**

There are many issues involved with whether a PSO can engage an active shooter to a "level of response expected." First, a PSO must have proper training for such situations, and currently they do not. FPS is working with NASCO and contractors to add active shooter training to the required PSO training. Second, PSO's are trained, instructed, and required by the contract to control access at their post, not to engage active shooters. While state law may provide PSO's (as state licensed armed officers) greater ability to engage an active shooter (or prevent an active shooter situation from occurring) FPS has made it clear that its guidance is preeminent, and thus disregarding the guidance would be a contract violation. Unless direct confrontation occurs or the PSO is directed by an authorized FPS representative, the PSO will adhere to Post Orders to shelter in-place to protect the building occupants and members of the public that may be at the building when the active shooter event occurs.

While there is no doubt that a PSO can and is expected to engage an active shooter that is in his line of sight/post area, and this has been the case with contract security officers at federal buildings, beyond that immediate area, FPS guidance/contract requirements would indicate that the PSO should not pursue and engage. A major underlying issue is also that while federal personnel may expect an armed PSO with a badge and uniform to pursue and engage an active shooter, PSO's are not law enforcement officials, and thus, unlike law enforcement, they and their employer do not have immunity from liability. PSO's need greater statutory authority to act to prevent/stop active shooter situations, such as the authority granted to contract security personnel who work at DOJ and DoE sites, and they need statutory liability protections. Congress should consider providing FPS with the authority to designate PSO's as limited law enforcement personnel on federal sites and provide contractors with the directives to properly train PSOs in the use of such authority, particularly with respect to engaging active shooters. However, specific training of the officers would also be needed to provide the requisite skills commensurate with this authority.

**5. Is there a lack of cooperation between FPS inspectors and the contract security officers they oversee? Is this an impediment to better cooperation and coordination between the two? What are the practical and potential implications for a dysfunctional working relationship between the two?**

There is not a lack of cooperation between FPS Inspectors and PSO's although it does vary. The key is the attitude of FPS Inspectors and FPS personnel to view PSO's and contractors as part of the team and generally the newer Inspectors are more willing to feel this way. Overall, cooperation has improved in the last couple years. However, some companies report very limited coordination between the HQ or Regional staff with the security company's management.

**6. Does FPS share its facility assessments with the security companies or the contract security officers? Can officers effectively be alert to threats to their facilities if the assessments are not shared, and how does this affect the ability of officers to carry out their duties?**

The answer to this question is an across the board "no." Some companies have seen reports dealing with building security when the FPS wanted to increase the PSO force and was designing the effort to justify the increase, but that level of information is not routinely shared. Other companies report that some tenants will not even tell the security contractor at the building what the security level is of the building even though security contractors sign an NDA. All companies agree that sharing the facility assessment with the security contractor can increase building security as PSO's could be more aware of

and trained on the specific threats identified in facility assessments. The findings of the assessments should be incorporated into PSO Post Orders which often are outdated and not tailored to the facility.

**7. Have efforts been made to update and standardize training for all contract security officers? Has an evaluation been made to identify mission critical skills for officers and has training been tailored to train those skills?**

In 2013, the ISC released its "Best Practice" for Armed Security Officers in Federal Facilities. This document will eventually be a required minimum Standard for all contract security officers. The ASO Standard was based on a job task analysis that FPS undertook when it decided several years ago to update its training and standards for PSO's which indeed looked to identify mission critical skills and physical requirements of PSO's and match them to training and medical/fitness requirements. The current FPS training requirements are virtually identical to the ISC Standard. FPS is now working with NASCO to standardize the provision of PSO training, the vast majority of which is provided by the contractor to its PSO's. While the training requirements may be the same, the lesson plans used are not, and FPS is in the process of creating a standardized PSO training lesson plan that all FPS contractors will use. NASCO agrees with this effort and has been assisting FPS. FPS also wants to have all contractor instructors certified, which NASCO agree with too. This standardization efforts should improve the training and performance of PSO's.

**8. What were the results of the "Red Team" exercises conducted against FPS facilities to evaluate the effectiveness of its facility security plan? What lessons were learned and what has been changed as a result of these exercises?**

FPS performs "red team" exercises (as part of "Operation Shield") at various facilities. Sometimes the red team exercise will also include immediate remedial training for PSO's to address weaknesses uncovered in the exercise and this is very helpful. However, it is labor intensive for FPS. Lessons learned from Operation Shield exercises can lead to changes in the training and operations. Red team exercises lose their effectiveness when, as is often the case, FPS does not provide any remedial training, and then does not inform the contractor of the results of the red team exercise until weeks or months after it occurred. This makes it virtually impossible for the contractor to take appropriate action, provide re-training, or use as a 'lessons learned' for other PSOs to prevent such penetrations in the future. Immediate feedback should be given to the contractor.

Contractors understand the value of red teaming and often will do such training scenarios on their own. However, FPS has a very uneven policy on such contractor exercises. Very successful company developed and executed Red Teaming was recently suspended in the National Capital Region without discussion or explanation. While they are being used in other regions across the country by the same providers, contractors are not currently authorized to engage in these activities in and around Washington, DC.

**Post-Hearing Questions for the Record**
**Submitted to David Wright**
**From Senator Thomas R. Carper**

**"The Navy Yard Tragedy: Examining Physical Security at Federal Facilities"**
**December 17, 2013**

1. At the hearing, you noted that Federal Protective Service personnel struggle to keep up with the amount and variety of work expected of them. Do you believe the Federal Protective Service should reexamine its workforce composition?

   Answer: Yes, I believe that FPS should reexamine its workforce composition after a thorough review of the Mission and what is expected from FPS. The increasing demands on the workforce for contract oversight and Facility Security Assessments (FSA's) without adequate tools and cooperation from GSA and other Federal Agencies places an enormous burden at the street level. The primary reason for the struggle is an inadequate number of field staff. In 2007, the reduction from 1,475 full time equivalent staff (FTE) to the current level of 1,371 FTE occurred. At the pre-2007 level, 1,309 FTE were authorized and assigned to the the eleven field regions. There are now approximately 1,120 FTE in the regions. Of course, a reduction of 15% in staffing without any material mission reduction has predictably increased the amount of work per Inspector. In these circumstances it should not be a surprise they struggle with the amount and variety of work expected of them. If additional field staffing were to be authorized, a future workforce composition of both Federal Police Officers and Inspectors in the 20 cities with the highest populations of federal workers in GSA facilities would improve efficiency. The Federal Police Officers, who are primarily dedicated to patrol and response duties and can also perform guard post inspections and would provide a baseline response level allowing Inspectors to dedicate more time to servicing their assigned facilities.

2. Do you believe the Federal Protective Service might be more effective if it received a direct appropriation, and could pay for the security measures it recommended, rather than request that tenant agencies pay for those security measures?

   Answer: The current method of collecting a basic security charge from all agencies and facilities for common service to fund FPS operating costs is inefficient. Charging other agencies for minimum security requirements inherently drives the priority implementation of security measures to only those who have discretionary funds available. I believe a direct appropriation of FPS operating costs certainly makes more sense than appropriating it to other agencies that must then transfer it to FPS. Direct appropriation of countermeasure funding would allow FPS to establish nationwide priorities based on risk to a facility rather than an agencies' ability to pay, and if appropriated at an adequate level, would be an improvement on the current system. Recurring Agency funding of specific security measures within their assigned space, such as Social Security Office contract guards, is effective and should continue.

3. At the hearing, NASCO has suggested that there is a conflict between federal guidance and state laws, when it comes to responding to an active shooter. Guidance distributed by the Federal Protective Service appears to limit the authority of armed guards protecting federal facilities, while some state laws may require armed guards intercede in the event of an active shooter. In other states, the law may constrain a security guard from taking certain actions, such as interdicting an active shooter. Do you believe guards should be empowered to interdict an active shooter?

   Answer:
   It is my understanding the contract guard vendors and guards must follow state and local restrictions on their ability to use force and any requirement to act. FPS post orders require action by the guards in a variety of situations, subject to legal restrictions. A Federal preemption of state or local laws limiting the response of guards in Federal facilities, who are acting as agents of FPS and following instructions provided by FPS, could be considered to ensure guards they are empowered to interdict threats entering the facility at their post. Guards can be trained to properly react and defend themselves and building occupants.

   Pursuit of an active shooter by contract guards causes operational and tactical issues with using individuals not trained as law enforcement officers to pursue an active shooter. In almost every case, active shooter response doctrine to locate and render an active shooter harmless requires more than one officer. Both local police and FPS receive regular training on the tactics and working together as team while contract guards do not. Additionally, in most cases an entry guard should remain at their post to prevent entry of other potential shooters, prevent escape of the shooter through containment, provide information to responding law enforcement, and ensure orderly evacuation of building occupants. The significant additional training required to integrate guards into teams of law enforcement officers may well be cost prohibitive in a private contract in this era of fiscal restraint.

   However, if contract guards at our Security Level 4 facilities and major Level 3 facilities were converted to Federal Police Officers a unified response would be more likely to be successful in our most critical facilities.

4. What three recommendations would you make to improve the effectiveness of the Federal Protective Service?

   Answer:
   Introduce and pass a Federal Protective Service Authorization Act that establishes FPS missions and codifies the proper roles of Facility Security Committees, Interagency Security Committee, tenant agencies and the General Services Administration.

   Restore the field staff to the levels authorized in FY 2007. Balance the workforce with Federal Police Officers to augment Inspectors with the patrol and response service.

Expeditious action to field an Interagency Security Committee compliant assessment tool that results in the more cost effective custom level of protection, rather than the baseline driven only by the general facility security level. Integrate specific threat ratings for the facility to guide the level of protection necessary to mitigate each threat. DHS Science and Technology have offered to assist FPS in this arena and I am confident that it can be accomplished.

An additional recommendation in the specific arena of "Active Shooter" incidents is to empower FPS to respond to federal facilities outside of the GSA control – regardless of rent.

David L. Wright
President
AFGE Local 918
Federal Protective Service Union

**Post-Hearing Questions for the Record**
**Submitted to Mr. David L. Wright**
**From Senator Jon Tester**

**"The Navy Yard Tragedy: Examining Physical Security for Federal Facilities"**
**December 17, 2013**

1. Mr. Wright, in your testimony you stated that, "the National Capital Region (NCR) Federal Protective Service (FPS) headquarters is barely two minutes from the Navy Yard—an expeditious FPS response was available but unused due to bureaucratic limitations." What exactly prevented the FPS from working quickly with local authorities during the Navy Yard shooting? What effect did this have on the apprehension of Aaron Alexis? Additionally, what red tape needs to be cut to make sure that the FPS can respond to an active shooter incident as soon as they are available?

Answer: A determination from the Office of General Counsel that fiscal law prevents FPS from providing services to Federal facilities that do not pay for basic services has been used as the reason for not responding. The Homeland Security Act gives FPS Officers jurisdiction at all Federal facilities, but because we are funded through security charges apparently we are not supposed to respond to other than General Services Administration owned or leased facilities.

I have no way of knowing how additional response by FPS would have specifically affected the interdiction of Aaron Alexis. That being said, at least several more teams of fully trained and fully equipped Federal officers would have been inside the Navy Yard that day within minutes, resolutely seeking an end to the terror.

The "red tape" can be cut by Congress clarifying that FPS may respond to any broadly defined emergency at any Federal facility.

David L. Wright
President
AFGE Local 918
Federal Protective Service Union

**Post-Hearing Questions for the Record**
**Submitted to David Wright**
**From Senator Tom Coburn**

**"The Navy Yard Tragedy: Examining Physical Security at Federal Facilities"**
**December 17, 2013**

1. Should the Facility Security Committee (FSC) make the final decision as to what security measures are adopted at a federal facility? Or, should the final decision be made by the Inspector, FPS, or GSA? Is the vetting process as currently structured too inefficient and burdensome and should the process be streamlined?

   Answer:
   There have been problems with FSC decisions on security measure implementation particularly clear documentation of when risk is accepted. Additionally many Inspectors have reported instances where the FSC merely lowered the Facility Security Level to avoid countermeasures. For FSL issues, the ISC provides for resolution only when two of the parties (GSA, tenant, or FPS) disagree. The Administrative Office of US Courts has stated "There is **no** ISC requirement that individual FSC members sign a document "accepting risk." Rather, the ISC standard is that if a proposal is voted down, it will be **noted** in the meeting minutes." This includes decisions to have an alarm or CCTV system, which non -law enforcement personnel are allowed to bypass screening for weapons and explosives, and other common sense protective measures. Noting in minutes rather than signing and requiring a reason appears designed to avoid accountability and responsibility.

   The current process should be streamlined. First a FSC should have to stand by its decision to accept risk by not implementing security measures, including the reason it is accepted, merely "noting" a vote not to implement appears to be designed to avoid accountability. A more workable structure would elevate final decisions on countermeasures and Facility Security Level to FPS Headquarters or to DHS. Under this process final decision could be elevated to FPS HQ who would attempt to resolve the issue with GSA and the tenant agencies. If it could not be resolved in 60 days FPS would make the decision. To discipline this system, all cases where FPS made the decision would be reported to the Homeland Security Committees of both the House and Senate.

2. How are FPS emergency response plans coordinated with other law enforcement personnel who are tenants in FPS-secured buildings? How are response efforts coordinated with state and local law enforcement? What is the mechanism used for coordination (MOU) and how frequently are exercises conducted?

   Answer:
   Every tenant is part of the response plan. Coordination depends on the facility and nature of their duties -- for example an ICE RAC or ERO office has armed officers assigned but most are in the field rather than the office. In Courthouses the USMS may be the first to respond from within the building with FPS and local police responding as well -- these situations are exercised and

coordination practiced, but there is no set schedule. In FBI and DEA field offices that are single tenant their reaction forces often may be the first active shooter response. In multi-tenant facilities they are typically responsible to initially secure their space and once coordination is in place to integrate them into the response. Practicing coordination as part of table top and other exercises is critical to prevent blue on blue accidents.

Response is coordinated with local police who have the ability to mass better than federal LE who are primarily engaged in field work. The level of coordination varies based on location. For example small standalone facilities like a Social Security Office would be just like any other commercial office in that city; however a Courthouse or large Federal building would involve orientation. I do not believe MOU's are used and in my experience may not be necessary - but in my position, I am not aware of all mechanisms that may be used. Director Patterson would be better equipped to respond to specific formal coordination documentation such as MOU.

Inspectors report that exercises are conducted and joint active shooter response training does occur in some areas. Table top exercises as part of the OEP process also occur. I am not aware of any set requirement for exercise frequency.

3. Is there a lack of cooperation between FPS inspectors and the contract security officers they oversee? Is this an impediment to better cooperation and coordination between the two? What are the practical and potential implications for a dysfunctional working relationship between the two?

   Answer:
   For the most part the cooperation is quite good. We are a team working to secure the facility. There is sometimes friction with contract companies, particularly when misconduct such as sleeping on duty is reported, and a contract security officer remains employed on the contract. The implications of a dysfunctional working relationship are failure of FPS to complete its mission. Good regional leadership and accountability of contractors are able to prevent a dysfunctional relationship from developing.

4. Does FPS share its facility assessments with the security companies or the contract security officers? Can officers effectively be alert to threats to their facilities if the assessments are not shared, and how does this affect the ability of officers to carry out their duties?

   Answer:
   As far as I am aware, FPS does not share its assessments with contract security forces, nor should it. The post orders, facility emergency plans and instructions provided to the contract guards are based on mitigating the facility vulnerabilities and integrating the security force countermeasure with other technical and physical countermeasures. Additionally, both the number of guard posts and duties are driven from the assessment and incorporated into the post orders. Guards and companies are routinely provided any threat alerts applicable to that facility and post orders are updated as changes occur and not less than annually. Providing information

tailored to their responsibilities and sharing of updated threat information on individuals or methods provides a better means of keeping guards alert to facility threats - rather than an assessment that may be three to five years old and contains information not relevant to the guard's duties.

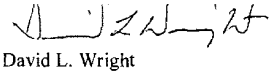
5. Have efforts been made to update and standardize training for all contract security officers? Has an evaluation been made to identify mission critical skills for officers and has training been tailored to train those skills?

   Answer:
   I understand FPS is engaged in an effort to increase standardization of training by developing lesson plans for guard company instructors to use when conducting training. The overall standards and knowledge have been standardized for some time. FPS provides through its Security Guard Manual the specific knowledge required and all guards must pass an FPS administered test on the manual prior to beginning work. FPS conducted training such as weapons detection is taught using a nationwide standardized lesson plan and examination – although I am confident there are severs shortcomings in some regions. Additionally, each semi-annual firearms qualification is required to be monitored by an FPS employee to ensure each guard qualifies according to the firing course in the contract.

6. What were the results of the "Red Team" exercises conducted against FPS facilities to evaluate the effectiveness of its facility security plan? What lessons were learned and what has been changed as a result of these exercises?

   Answer:
   I am not officially aware of national results of covert testing for weapons detection. Since both scenarios and specific results are sensitive For Official Use Only information, Director Patterson can answer more fully than I. I do know that after each test an after action review is conducted, issues are mitigated and typically guards who fail are retrained or removed by their employer. Inspectors and Agents have reported that the more contract guards are tested the better they perform. I would recommend more tests using a more full range of scenarios be conducted.

   That all being said, I have heard much anecdotal evidence from street level Inspectors, Police Officers and Special Agents involved in the testing - that many results are "dismal".



David L. Wright
President
AFGE Local 918
Federal Protective Service Union

○