AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

ARE FEDERAL AND POSTAL EMPLOYEES SAFE AT WORK?

HEARING

BEFORE THE

SUBCOMMITTEE ON FEDERAL WORKFORCE, POSTAL SERVICE, AND THE DISTRICT OF COLUMBIA

OF THE

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

HOUSE OF REPRESENTATIVES

ONE HUNDRED ELEVENTH CONGRESS

SECOND SESSION

MARCH 16, 2010

Serial No. 111–69

Printed for the use of the Committee on Oversight and Government Reform

Available via the World Wide Web: http://www.gpoaccess.gov/congress/index.html
http://www.house.gov/reform

U.S. GOVERNMENT PRINTING OFFICE

57–976 PDF WASHINGTON : 2010

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 OVERSIGHT AND GOVERNMENT REFORM

EDOLPHUS TOWNS, New York, *Chairman*

PAUL E. KANJORSKI, Pennsylvania
CAROLYN B. MALONEY, New York
ELIJAH E. CUMMINGS, Maryland
DENNIS J. KUCINICH, Ohio
JOHN F. TIERNEY, Massachusetts
WM. LACY CLAY, Missouri
DIANE E. WATSON, California
STEPHEN F. LYNCH, Massachusetts
JIM COOPER, Tennessee
GERALD E. CONNOLLY, Virginia
MIKE QUIGLEY, Illinois
MARCY KAPTUR, Ohio
ELEANOR HOLMES NORTON, District of Columbia
PATRICK J. KENNEDY, Rhode Island
DANNY K. DAVIS, Illinois
CHRIS VAN HOLLEN, Maryland
HENRY CUELLAR, Texas
PAUL W. HODES, New Hampshire
CHRISTOPHER S. MURPHY, Connecticut
PETER WELCH, Vermont
BILL FOSTER, Illinois
JACKIE SPEIER, California
STEVE DRIEHAUS, Ohio
JUDY CHU, California

DARRELL E. ISSA, California
DAN BURTON, Indiana
JOHN M. MCHUGH, New York
JOHN L. MICA, Florida
MARK E. SOUDER, Indiana
TODD RUSSELL PLATTS, Pennsylvania
JOHN J. DUNCAN, JR., Tennessee
MICHAEL R. TURNER, Ohio
LYNN A. WESTMORELAND, Georgia
PATRICK T. MCHENRY, North Carolina
BRIAN P. BILBRAY, California
JIM JORDAN, Ohio
JEFF FLAKE, Arizona
JEFF FORTENBERRY, Nebraska
JASON CHAFFETZ, Utah
AARON SCHOCK, Illinois

RON STROMAN, *Staff Director*
MICHAEL MCCARTHY, *Deputy Staff Director*
CARLA HULTBERG, *Chief Clerk*
LARRY BRADY, *Minority Staff Director*

SUBCOMMITTEE ON FEDERAL WORKFORCE, POSTAL SERVICE, AND THE DISTRICT OF COLUMBIA

STEPHEN F. LYNCH, Massachusetts, *Chairman*

ELEANOR HOLMES NORTON, District of Columbia
DANNY K. DAVIS, Illinois
ELIJAH E. CUMMINGS, Maryland
DENNIS J. KUCINICH, Ohio
WM. LACY CLAY, Missouri
GERALD E. CONNOLLY, Virginia

JASON CHAFFETZ, Utah
ANH "JOSPEH" CAO, Louisiana
MARK E. SOUDER, Indiana
BRIAN P. BILBRAY, California

WILLIAM MILES, *Staff Director*

CONTENTS

	Page
Hearing held on March 16, 2010	1
Statement of:	
Goldstein, Mark, Director, Physical Infrastructure, U.S. Government Accountability Office; Steven Miller, Deputy Commissioner for Services and Enforcement, Internal Revenue Service; Sue Armstrong, Acting Deputy Assistant Secretary, Office of Infrastructure Protection and Gary Schenkel, Director, Federal Protective Service, National Protection and Programs Directorate, U.S. Department of Homeland Security; and Guy Cottrell, Deputy Chief Postal Inspector, U.S. Postal Inspection Service	17
Armstrong, Sue	39
Cottrell, Guy	51
Goldstein, Mark	17
Miller, Steven	34
Schenkel, Gary	40
Kelley, Colleen, national president, National Treasury Employees Union; Jon Adler, national president, Federal Law Enforcement Officers Association; and David Wright, president, Local 918, American Federation of Government Employees	70
Adler, Jon	79
Kelley, Colleen	70
Wright, David	86
Letters, statements, etc., submitted for the record by:	
Adler, Jon, national president, Federal Law Enforcement Officers Association, prepared statement of	82
Armstrong, Sue, Acting Deputy Assistant Secretary, Office of Infrastructure Protection and Gary Schenkel, Director, Federal Protective Service, National Protection and Programs Directorate, U.S. Department of Homeland Security, prepared statement of	42
Chaffetz, Hon. Jason, a Representative in Congress from the State of Utah, prepared statement of	10
Connolly, Hon. Gerald E., a Representative in Congress from the State of Virginia, prepared statement of	15
Cottrell, Guy, Deputy Chief Postal Inspector, U.S. Postal Inspection Service, prepared statement of	53
Cummings, Hon. Elijah E., a Representative in Congress from the State of Maryland, prepared statement of	107
Goldstein, Mark, Director, Physical Infrastructure, U.S. Government Accountability Office, prepared statement of	19
Kelley, Colleen, national president, National Treasury Employees Union, prepared statement of	72
Lynch, Hon. Stephen F., a Representative in Congress from the State of Massachusetts:	
Prepared statement of	8
Prepared statement of Mr. Thompson and a DOD employee	2
Miller, Steven, Deputy Commissioner for Services and Enforcement, Internal Revenue Service, prepared statement of	36
Wright, David, president, Local 918, American Federation of Government Employees, prepared statement of	88

ARE FEDERAL AND POSTAL EMPLOYEES SAFE AT WORK?

TUESDAY, MARCH 16, 2010

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON FEDERAL WORKFORCE, POSTAL SERVICE, AND THE DISTRICT OF COLUMBIA,
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM,
Washington, DC.

The subcommittee met, pursuant to notice, at 2:10 p.m. in room 2154, Rayburn House Office Building, Hon. Stephen F. Lynch (chairman of the subcommittee) presiding.

Present: Representatives Lynch, Norton, Cummings, Connolly, and Chaffetz.

Staff present: William Miles, staff director; Jill Crissman, professional staff; Rob Sidman, detailee; Dan Zeidman, deputy clerk/legislative assistant; Howard Denis, minority senior counsel; and Alex Cooper, minority professional staff member.

Mr. LYNCH. Good afternoon. The Subcommittee on the Federal Workforce, Postal Service, and District of Columbia hearing will now come to order. I apologize for the brief delay. We have a lot going on here today. Members will be coming in and leaving periodically. Unfortunately, we seem to schedule everything at the same time here in light of the work that needs to be done.

I want to welcome my friend and ranking member, Mr. Chaffetz from Utah, and members of the subcommittee hearing, witnesses, and all those in attendance.

In light of the recent attacks and violent outbursts against Federal workers and facilities, I have called today's hearing to examine Federal and Postal employee workplace security.

The Chair, ranking member, and the subcommittee members will each have 5 minutes to make opening statements, and all Members will have 3 days to submit statements for the record.

I would also like to ask unanimous consent that the testimony of Congressman Benny Thompson, who is our chairman of the Committee on Homeland Security, and that of a DOD employee, be submitted for the record.

Hearing no objection, so ordered.

[The prepared statements of Mr. Thompson and the DOD employee follow:]

BENNIE G. THOMPSON, MISSISSIPPI
CHAIRMAN

PETER T. KING, NEW YORK
RANKING MEMBER

Bennie G. Thompson

One Hundred Eleventh Congress
U.S. House of Representatives
Committee on Homeland Security
Washington, DC 20515

Statement for the Record for Chairman Bennie G. Thompson

Chairman, Committee on Homeland Security

Hearing entitled, "Federal Employee Workplace Security"

Before the

Committee on Oversight and Government Reform

Subcommittee on Federal Workforce, Postal Service and the District of Columbia

March 16, 2010

I would like to thank Chairman Lynch for permitting me to submit a statement for the record for today's hearing entitled, "Federal Employee Workplace Security." Today's hearing on the safety and security of Federal buildings is critically important.

In the last ten years there have been several major attacks on Federal facilities and the employees therein. Those attacks have led to the unfortunate deaths of Federal employees and innocent civilians. While all are familiar with the heinous terrorist attacks of September 11, 2001, other fatal attacks have not been as well publicized. For instance, the anthrax letters sent to the offices of two U.S. Senators in 2001, led to the death of two U.S. Postal Service employees; the 2005 incident at the Seattle Federal Courthouse when a man was shot and killed by police after attempting to enter and threaten the facility with an inert grenade; the 2007 incident at the Lyndon B. Johnson Space Center in which a NASA contract engineer shot and killed a coworker and took another hostage before ultimately taking his own life; and the 2009 attack at the U.S. Holocaust Museum, which led to the death of a guard. This year, we have already witnessed a fatal shooting at the Lloyd D. George Federal Courthouse in Las Vegas, Nevada; a fatal attack against an IRS building in Austin, Texas; and a shooting incident outside the Pentagon that resulted in the death of the assailant. Despite these incidents, the Federal government's posture regarding the protection and security of Federal facilities has not significantly changed.

As Chairman of the Committee on Homeland Security, I am closely monitoring the role the Federal Protective Service plays in the current federal security climate. As a part of the Department of Homeland Security, the Federal Protective Service (FPS) is charged with protecting Federal government property, personnel, visitors, and customers at over 9,000 Federal facilities across the nation.

I think most taxpayers would assume that this important mission—guarding Federal facilities—would be accomplished by Federal employees. But that assumption would be incorrect. The Federal Protective Service relies entirely on a contract guard force to perform the physical security at these Federal facilities where members of the public—taxpayers—come to seek information and assistance from their government.

Supervised by a small number of Federal Protective Service Inspectors who are trained Federal law enforcement officers, these contract guards do not receive standardized training and do not have any law enforcement authority.

The Committee on Homeland Security has had several hearings on the Federal Protective Service. Thos hearings led to internal reforms by FPS which resulted in improved accounting procedures, a revamping of a backlogged payment process, and a resolution of a long-standing deficit. But after getting the financial house in order, it is time to focus on FPS' protection mission. As revealed in a hearing held by the Committee on Homeland Security on November 18, 2009, a GAO investigation revealed that undercover inspectors were able to successfully carry unassembled explosive devices through security checkpoints staffed by contract guards at 100% of the facilities tested.

These security lapses at Federal facilities must not be permitted to continue. In April, the Committee on Homeland Security will hold an oversight hearing to directly address the issue of the Federal Protective Service's ability to provide adequate security at Federal facilities. The Committee is also preparing legislation to improve FPS. Given the nature of the risks we face and the importance of Federal facilities and all who work and visit them, I don't think we can rule out the possibility that the best way to improve the Federal Protective Service would be to federalize its guard workforce.

Mr. Chairman, the lack of effective security at Federal facilities is simply unacceptable. Federal employees and civilians deserve to have the utmost confidence that they are being kept as safe as possible when working in or visiting a federal facility.

Chairman Lynch, I thank you for your leadership on this issue and look forward to working with you in assuring the safety of Federal facilities, the Federal workforce and every taxpayer who comes to a federal building to seek information or assistance.

March 14, 2010

The Honorable Stephen F. Lynch
Chair, Subcommittee on Federal Workforce, Postal Service, and the District of Columbia
Committee on Oversight and Government Reform
U.S. House of Representatives
2157 Rayburn House Office Building
Washington, D.C. 20515

Dear Chairman Lynch and Members of the Subcommittee:

I understand that you are holding an Oversight Hearing on Tuesday, March 16, 2010, to examine Federal Employee Workplace Safety and Security workplace violence. As a victim of workplace violence, I would like to submit a statement for the record on workplace intimidation, bullying, harassment, and violence I suffered; the lack of response from management, and relentless retaliation on me for my reporting the incident.

My name is Christi Carter and I work at the Pentagon as an Air Force civilian. In October 2009 I notified senior management at the flag officer level of an issue involving workplace bullying, harassment, and even assault by a co-worker; and subsequent intimidation by mid-level management to cover up the behavior. You see I was bullied, harassed, and intimidated for many months by another federal worker. The bullying escalated over time until the co-worker kicked me (assaulted me) in anger. Management did nothing. They laughed, scoffed, and said it was no big deal. When I reported the assault to Equal Employment Opportunity (EEO) and Pentagon Force Protection Agency (PFPA) authorities, senior management initiated a veiled campaign to discredit me, took deliberate action to punish me for reporting the incident, and intimidated all personnel in the Directorate; thus affecting their willingness to make candid statements about the incident in question—and the toxic culture in the organization in general. From a federal workforce perspective, management simply failed to act following an assault on one employee by another. Management then attempted to hide the lack of action by being deceptive and coercive; while initiating a campaign to discredit and punish me for reporting the events; thus creating fear in the hearts and minds of all federal workers under the organization. The lack of public law addressing, forbidding, and offering recourse for workplace intimidation, bullying, harassment, and other forms of less discernable workplace violence contributed to my situation.

The retaliation from senior management was visceral. Management attacked me like a pack of wolves and set into motion a series of covert, subversive efforts and communications between senior military officers to cover for each other and thwart my efforts for assistance from the Department of the Air Force and the Secretary of Defense. On January 21, 2010 I sent a memorandum (enclosed with this statement) to the Secretary of Defense requesting his help. I asked the Secretary of Defense for help because each attempt I made for help within the Department of the Air Force was intercepted and re-routed back inside the circle of control and influence of those involved in covering up the lack of action by management and subsequent

retaliation. Within a week of sending the memorandum to the Secretary of Defense, the memorandum was once again re-routed "inside" the Department of the Air Force for resolution; and within a week of that was quickly routed back inside the circle of control and influence of those involved. In fact, evidence suggests the Department of the Air Force Inspector General office may have leaked details of the memorandum back to senior management directly involved in the incident. The retaliation against me by management continues as of the date of this statement. The vicious circle and cycle of retaliation and cover-up has taken a huge emotional toll on me and my family. It has caused me bouts of depression and emotional distress.

Members of the federal workforce spend thousands and hundreds of thousands of dollars each year in attorney and court fees to defend themselves against federal departments that should be required by public law to protect them from events such as mine. They are forced into the situation because of a lack of public laws to protect employees from the less discernable forms of workplace violence such as: bullying, intimidation, and harassment. While current EEO laws are fairly comprehensive and have considerable depth written into their language; there are no laws in this country to protect the federal workforce from specifically less discernable forms of workplace violence such as: bullying, intimidation, and harassment. Although the Office of Personnel Management has published policies against such workplace harassment, the policies are not linked to public law; unless loosely tied to a secondary EEO law or law against retaliation for an EEO complaint. In addition, OPM guidance makes the publication of workplace violence policy statements by each agency optional. It is widely known in legal circles that this is a very difficult area to legislate and as such remains a gapping hole in legal federal protections for employees. I would suggest that to do nothing...to have no public laws specifically prohibiting workplace bullying, intimidation, and harassment indirectly condones these forms of workplace violence and accepts that such activity can and often does progress into an episode of assault and retaliation for reporting such events.

> [My] incident of workplace violence may not involve billions of dollars for a weapons platform; or repeal of NSPS which affects 226,000 civilian employees; or expansion of a Family Medical Leave Act or other workforce-wide legislative act affecting all federal civilians—it may have neither the scope nor fiscal affect of most issues confronted by the committee or sub-committee. In fact on the surface it may appear to affect only [me]. But below the surface it has a caustic and destructive effect; you see squashing an employee's right and desire to ask for help damages the very fabric of fair and equal employment that over time compromises every worker in the federal workforce. John Stuart Mill, in his work, On Liberty, was the first to recognize that the absence of liberty produces coercion and the arbitrary exercise of authority. The affect of multiple echelons of management covering for each other, smothering the truth, and preventing others from exposing injustices threatens the very liberty that this country was founded on. The level of arrogance and degree of coercive tactics that have been used by management against full disclosure and against me personally sacrifices the core values all...leaders should hold dear: Integrity, service before self, and excellence in all we do. (Mark Carter, Feb 21, 2010 Memo to Senator Akaka staff)

I have included for the record the memorandum to the Secretary of Defense which provides a more detailed summary of events in my case.

> James Madison, our fourth President once said about liberty, "Liberty may be endangered by the abuse of liberty, but also by the abuse of power." There has clearly been a covert abuse of power in my incident. The issue may affect just one person today, but if this abuse of power—the abuse of power that creates fear and intimidation to block free thought and expression—goes unchecked, the result will be a corrosive affect on many more federal employees in the future. (Mark Carter, Feb 21, 2010 Memo to Senator Akaka staff)

I have secured an attorney at significant expense to myself, but it is unfortunate when federal employees are forced to hire an attorney to protect themselves from federal institutions that should be mandated by public law to protect them. I once again urge this committee to consider the need for legislation to address workplace violence; and more specifically bullying, harassment, and intimidation in the federal workplace; and join me to stand for what is right, and just, and ethical in the treatment of one of our nations most valued contributors to our democracy--our federal employees.

Sincerely and with respect,

Christi Carter

Mr. LYNCH. Ladies and gentlemen, in recent weeks we have witnessed several brutal attacks and violent outbursts against Federal workers and facilities, which is why I have called today's hearing. Tragically, in 2010, alone, a U.S. court security officer in Las Vegas, and an IRS manager in Austin, TX, have lost their lives, while several law enforcement personnel, including a deputy U.S. Marshall and members of the Pentagon Force Protection Agency, have been injured in the line of duty.

Given the rise of anti-Government feeling, as notably reported in the Southern Poverty Law Center's 2009 Report entitled, "The Second Wave," I believe that, as chairman of the subcommittee, I have a duty to examine how well positioned Federal agencies and the Postal Service are for similar events.

Today's hearing will also allow us to discuss what agencies are doing to provide comprehensive training and guidance to employees on how to respond to such threats and scenarios. It is one thing to hear about agencies wrestling with how to afford purchasing expensive security countermeasures, but it is quite a different matter to listen to Federal employees recount the lack of emergency preparedness of a particular office. It may be that an emergency plan exists, but if the individual workers aren't familiar with it and are not even practicing any type of evacuation drills, then what type of outcome can we expect if and when disaster strikes.

An important item to note here is that the Federal and Postal employees warrant our respect. For some to look at the violence directed against IRS employees and to try to justify that deliberate intent to murder other human beings is simply inexcusable and unacceptable. Our Nation's public servants deserve nothing less than our full support, and to know that all of us, from the President to Congress, are grateful for their work and assistance in helping us govern our Nation.

More importantly, our Federal employees need to know that we will do everything possible to keep them safe while they are at the workplace and away from their families.

Today's hearing will provide us with the opportunity to hear from the IRS and its employee representatives concerning both the immediate and long-term impact of the February 18th attack in Austin. Additionally, we will hear from the Department of Homeland Security about its ongoing activities in the Federal building security area, as well as from the U.S. Postal Service's Inspection Service.

It is my hope that the testimony and feedback we receive from today's witnesses will provide the subcommittee with precise guidance and direction.

Again, I thank each of you for being with us this afternoon and I look forward to your participation.

[The prepared statement of Hon. Stephen F. Lynch follows:]

STATEMENT OF CHAIRMAN STEPHEN F. LYNCH

SUBCOMMITTEE ON FEDERAL WORKFORCE, POSTAL SERVICE, AND THE DISTRICT OF COLUMBIA HEARING ON

"Federal Employee Workplace Security"
Tuesday, March 16th, 2010

Ladies and Gentlemen, in recent weeks, we have witnessed several brutal attacks and violent outburst against federal workers and facilities, which is why I have called today's hearing. Tragically, in 2010 alone, a U.S. court security officer in Las Vegas and an IRS manager in Austin, Texas, have lost their lives, while several law enforcement personnel – including a deputy U.S. Marshal and members of the Pentagon's Force Protection Agency – have been injured in the line of duty.

Given the rise of anti-government feelings, as notably reported in the Southern Poverty Law Center's 2009 report entitled, *The Second Wave*, I believe that as Chairman of this Subcommittee, I have a duty to examine how well-positioned federal agencies and the Postal Service are for similar events. Today's hearing will also allow us to discuss what agencies are doing to provide comprehensive training and guidance to employees on how to respond to such threats and scenarios. It's one thing to hear about agencies wrestling with how to afford purchasing expensive security countermeasures – but it's quite a different matter, to listen to federal employees recount the lack of emergency preparedness of a particular office – it may be that as an agency an emergency plan exists, but if the individual workers aren't familiar with it, and are not even practicing any type of evacuation drills, what kind of outcome can we expect if and when disaster strikes?

An important item to note here is that federal and postal employees warrant our respect. For some to look at the violence directed against IRS employees and to try and justify the deliberate intent to murder other human beings – is inexcusable and unacceptable. Our nation's public servants deserve nothing less than our full support – and to know that all of us – from the President to Congress – are grateful for their work and assistance in helping us govern our nation. More importantly, our federal employees need to know that we will do everything possible to keep them safe while at the workplace and away from their families.

Today's hearing will provide us with the opportunity to hear from the IRS and its employee representatives concerning both the immediate and long-term impact of the February 18th attack in Austin. Additionally, we will hear from the Department of Homeland Security about its ongoing activities in the federal building security area, as well as from the U.S. Postal Service's Inspection Service. It is my hope that the testimony and feedback we receive from today's witnesses will provide the Subcommittee with precise guidance and direction. Again, I thank each of you for being with us this afternoon, and I look forward to your participation.

Mr. LYNCH. I now yield 5 minutes to our ranking member, Mr. Chaffetz.

Mr. CHAFFETZ. Thank you, Mr. Chairman. And thank you for holding this important hearing. I appreciate all of those witnesses that have come to testify today.

Needless to say, we want to make sure that every Federal employee and the public who is engaging with the Federal Government at all times is as safe as possible. People should deserve and expect to work in a safe environment. We need to constantly evaluate the standards and procedures, so I think this hearing is particularly appropriate at this time. I look forward to hearing the discussion.

For those very few but important men and women who have been on the wrong end of this violence, our hearts, thoughts, and prayers go out to those people.

We need to continue to strive to improve and make the workplace as safe as we can, but also accessible, at the same time.

I look forward to this hearing. I thank, again, the chairman for holding it and yield back the balance of my time.

[The prepared statement of Hon. Jason Chaffetz follows:]

OPENING STATEMENT OF JASON CHAFFETZ
RANKING MEMBER
SUBCOMMITTEE ON FEDERAL WORKFORCE, POSTAL SERVICE, AND THE DISTRICT OF COLUMBIA
MARCH 16, 2010

- **Thank you Mr. Chairman for holding this important hearing to examine safety and security issues in Federal buildings.**

- **Federal employees are on the front line in protecting us against ongoing threats to the American people and our way of life.**

- **There is a constant need to evaluate standards and protocols. Coordination is essential in order to achieve the highest level of security for all.**

- **It's not very long ago that access to government offices was as simple as walking through an entrance. But terrorists of all kinds have over time created a daunting, and often unnerving gauntlet for us all to endure.**

- **An entire generation has now grown up to whom this has become the norm, a chilling daily reminder of the real threats we face.**

- **This subcommittee has jurisdiction for both federal workforce and postal service issues. Looking at postal facilities alone, there are more retail locations than for McDonalds, Starbucks, Walgreens, and Walmart combined! Postal workers represent around 25% of all**

government workers, and in 2001 sustained casualties as a result of the anthrax attacks.

- **The safety of federal employees is a priority for all of us.**

- **Our government workers are to be commended for their courage in the face of constant danger. Their high degree of training has resulted in swift, measured, and appropriate responses to many horrific incidents, mitigating what could otherwise have been even more tragic outcomes. We are grateful to our government workers for their effective response, and want to commend them all for their valiant and ongoing efforts.**

- **I look forward to the testimony of all the government and labor witnesses who will be appearing before us this afternoon.**

- **Thank you again Mr. Chairman.**

Mr. LYNCH. I thank the gentleman.

I would now like to yield 5 minutes to Ms. Eleanor Holmes Norton, the Congresswoman from the District of Columbia, who has also been at the forefront of this issue, because of the number of Federal facilities in her District, for a long, long time.

Ms. Norton.

Ms. NORTON. Thank you, Mr. Chairman. I am especially appreciative that you have called this hearing so soon after the attacks in Austin and right here in the National Capital Region, first with the IRS in Austin, and here in this region at the Pentagon.

Mr. Chairman, in post-9/11 America there has to be a renewed appreciation for Federal workers and the kind of hammering of civil servants stopped. They recognize how important was the work of those who are spread across our Government. It is very disturbing to see the uptick in attacks on Federal employees once again.

Mr. Chairman, during the last 10 years or so, the Federal Protective Service was literally drained of employees, and it got so bad that we asked and the Appropriations Committee mandated that a certain floor of Federal Protective Service guards and officers be retained. There was the notion that all you needed was security guards, you didn't even need a Federal Protective Service, even though that is the oldest of the police forces in the Federal Government. It was very disconcerting.

Mr. Chairman, I chair a subcommittee with jurisdiction over Federal construction and leasing, and have some jurisdiction over the Federal Protective Service in that regard, and I am a member of the Homeland Security Committee, and if I may say so, Mr. Chairman, the so-called Interagency Security Committee is something of a joke. This is a committee that is supposed to sit and coordinate security for Federal buildings, sites, and employees.

But to show you just how ineffective is the protection of Federal workers, take a building like the new Transportation, not so old, maybe about 5 years old, the new Transportation Department. That is not a high security building. Mr. Chairman, when my staff, with their congressional tags on, have gone to that building, they can't get in there. Somebody in the agency has to stop her work and come down in order for them to enter the premises, even though these people have the credentials of the U.S. Capitol on them.

That is what you have at one end, in a building that we do not think Al Qaeda is much looking for. At the other end, we have more sensible security in some other parts of the Government. How could this be? The reason it is this way, Mr. Chairman, is that security gets decided on the premises. No matter what they tell you, it is some GS–9 somewhere who sits with a committee and decides who will come into this agency or not, and the rest of it.

And if it goes up to the Secretary and the Secretary says, that is fine with me, well then even staff from the Capitol can't get in. If it is someone who has a more even sense of security and what it means, maybe they will. But I can tell you this, Mr. Chairman: I have seen security in buildings that I think Al Qaeda would be far more interested in entering that do not have the security of the Transportation Department.

We have had hearings ourselves on it. I would like very much for my subcommittee, for the Homeland Security Committee, and you, Mr. Chairman, to get together so that we can, in a concerted way, make the Federal Government protect Federal employees by having one standard that is minimal and then tailor it to other parts of the Government which may require more or less.

Again, I very much appreciate the respect you show for the safety of Federal employees by holding such a prompt hearing here this afternoon.

Mr. LYNCH. Thank you. Certainly we are looking for best practices to be adopted.

The Chair now recognizes the gentleman from Virginia, Mr. Connolly, for 5 minutes.

Mr. CONNOLLY. I thank you, Chairman Lynch, and thanks so much for holding this very important hearing.

Last year we have witnessed a rise in violent rhetoric by extremist groups in America; therefore, we must consider not only those infrastructure improvements to protect Federal employees, to protection Federal employees from terrorism, but also the manner in which we may exercise justification of violence from public discourse.

Less than 1 month ago, Andrew Joseph Stack intentionally crashed his small plane into a Federal building in Austin, TX that included offices of the Internal Revenue Service filled with Federal employees. This terrorist attack killed Vernon Hunter, a Federal employee who previously served two terms overseas in the Armed Forces.

Incredibly, some political figures offered a tacit defense of that terrorist attack. One such individual was recorded as saying, "I think if we had abolished the IRS back when I first advocated it, he wouldn't have had a target for his airplane." Previously, he told the Conservative Political Action Conference that he empathized with the terrorist who flew his plane into the Federal building in Austin. This defense of terrorism is remarkable, because under this logic the victims of terrorism bear the responsibility of the terrorist attack.

This implicit figure's reprehensible defense of terrorism is consistent with the disturbing trend of violent, anti-government extremism we have seen in our country all too often. According to the Southern Poverty Law Center, the slaughter engineered by Timothy McVeigh and Terry Nichols, men steeped in the conspiracy theories and white hot fury of the American radical right, marked the opening shot on a new kind of domestic political extremism, a revolutionary ideology whose practitioners do not hesitate to carry out attacks directed at entirely innocent victims, people selected essentially at random, to make a political point.

Since 1995, there have been over 75 violent attacks by domestic terrorists like Timothy McVeigh and Andrew Joseph Stack, including the 1996 bombing at the Atlanta Olympics by anti-abortion fanatic Eric Rudolph and the 2009 murder of a guard at the Holocaust Museum by anti-Semite James von Brunn. It would be reprehensible enough for anyone to endorse violence generally, but even worse is endorsement of violence in response to non-violent

policies with which one might disagree, such as the terrorist attack against the IRS to express tax grievances.

Terrorism can never be condoned. Violence against Federal workers and installations is never acceptable. Those who, for cheap political pandering, find themselves justifying it most assuredly have the blood of its innocent victims, like Vernon Hunter, on their hands.

Thank you, Mr. Chairman.

[The prepared statement of Hon. Gerald E. Connolly follows:]

Opening Statement of Congressman Gerald E. Connolly

Federal Employee Workplace Safety

Subcommittee on Federal Workforce, Postal Service, and the District of Columbia

March 16th, 2010

Thank you, Chairman Lynch for holding this important hearing. Over the last year we have witnessed a rise in violent rhetoric by extremist groups in America. Therefore, we must consider not only those infrastructure improvements that can protect federal employees from terrorism, but also the manner in which we may exorcise justification of violence from public discourse.

Less than one month ago, Andrew Joseph Stack intentionally crashed his small plane into a federal building in Austin, Texas, that included offices of the Internal Revenue Service. This terrorist attack killed Vernon Hunter, a 27 year federal employee who previously served two tours overseas in the armed forces. Incredibly, some political figures offered a tacit defense of this terrorist attack. One such individual was recorded saying "I think if we'd abolished the IRS back when I first advocated it, he wouldn't have a target for his airplane." Previously, he told the Conservative Political Action Conference that he "empathized" with the terrorist who flew his plane into the federal building in Austin. This defense of terrorism is remarkable because under this logic the victims of terrorism bear the responsibility for a terrorist attack.

This political figure's reprehensible defense of terrorism is consistent with a disturbing trend of violent anti-government extremism in America. According to the Southern Poverty Law Center:

> *The slaughter engineered by Timothy McVeigh and Terry Nichols, men steeped in the conspiracy theories and white-hot fury of the American radical right, marked the opening shot in a new kind of domestic political extremism — a revolutionary ideology whose practitioners do not hesitate to carry out attacks directed at entirely innocent victims, people selected essentially at random to make a political point. After Oklahoma, it was no longer sufficient for many American right-wing terrorists to strike at a target of political significance — instead, they reached for higher and higher body counts, reasoning that they had to eclipse McVeigh's attack to win attention.*

Since 1995, there have been over 75 violent attacks by domestic terrorists like Timothy McVeigh and Andrew Joseph Stack, including the 1996 bombing at the Atlanta Olympics by anti-abortion fanatic Eric Rudolph and the 2009 murder of a guard at the Holocaust museum by anti-Semite James Von Brunn.

It would be reprehensible enough for anyone to endorse violence generally, but even worse is endorsement of violence in response to non-violent policies with which one might disagree, such as a terrorist attack against the IRS to express tax grievances. Terrorism can never be condoned. Violence against federal workers and installations is never acceptable. Those who, for cheap political pandering, find themselves justifying it most assuredly have the blood of its innocent victims like Vernon Hunter on their hands.

Mr. LYNCH. I thank the gentleman.

The committee will now hear testimony from today's witnesses. It is the standard policy of this committee that all witnesses who are to offer testimony shall be sworn. Could I ask you to all stand and raise your right hands?

[Witnesses sworn.]

Mr. LYNCH. Let the record indicate that all the witnesses have each answered in the affirmative.

What I will do is I will offer a brief introduction of each of our witnesses, and then we will afford each an opportunity to testify for 5 minutes.

First of all, Mr. Mark Goldstein is the Director of Physical Infrastructure Issues at the U.S. Government Accountability Office. Mr. Goldstein is responsible for the Government Accountability Office work in the areas of Government property and telecommunications, and has held other public sector positions, serving as deputy director and chief of staff to the District of Columbia Financial Control Board, and as a senior staff member of the U.S. Senate Committee on Governmental Affairs. Mr. Goldstein is also an elected fellow of the National Academy of Public Administration.

Mr. Steven Miller is Deputy Commissioner for Services and Enforcement, providing direction and oversight for all major decisions affecting the four taxpayer-focused Internal Revenue Service divisions: wage and investment, large and mid-sized business, all business, self-employed and tax-exempt and government entities. He is also responsible for the IRS Criminal Investigation Division, which investigates income tax evasion, the IRS Office of Professional Responsibility, which administers the laws governing the practice of tax professionals before the IRS, and the IRS whistleblower office, which receives information on tax cheating.

Ms. Sue Armstrong was named the Acting Deputy Assistant Secretary in September 2009 of the Office of Infrastructure Protection, a division of the National Protection and Programs Directorate at the Department of Homeland Security. In this capacity, she supports the Assistant Secretary in leading the coordinated national effort to reduce the risk to the Nation's critical infrastructure and key resources posed by acts of terrorism, and increasing the Nation's preparedness and rapid recovery in the event of an attack, natural disaster, or other emergency.

Mr. Gary W. Schenkel was appointed Director of the Federal Protective Service, a Division of the National Protection and Programs Directorate at the Department of Homeland Security, in March 2007. A retired Marine Corps lieutenant colonel, Schenkel has significant leadership and experience in a wide range of arenas, including organizational transformation efforts, security planning for public facilities, logistical planning and execution, and business administration.

Mr. Guy Cottrell joined the Postal Service in 1987 as a letter carrier in New Orleans, LA. In 2008 Mr. Cottrell was asked to come to National Headquarters to lend his expertise and leadership to the Chief Postal Inspector's role as Chief Security Officer of the Postal Service as Inspector in Charge of the Secretary and Crime Prevention Communications Group. In 2009, Mr. Cottrell was se-

lected as Deputy Chief Inspector, Headquarters Operation, with oversight of all Postal Service national security programs.

Welcome to all of our witnesses.

Mr. Goldstein, you are now recognized for 5 minutes.

Let me just explain that box in the middle of the table will show green while your time is proceeding. It will show yellow when it is time to wrap up, and then red when you should probably stop offering testimony.

Mr. Goldstein.

STATEMENTS OF MARK GOLDSTEIN, DIRECTOR, PHYSICAL INFRASTRUCTURE, U.S. GOVERNMENT ACCOUNTABILITY OFFICE; STEVEN MILLER, DEPUTY COMMISSIONER FOR SERVICES AND ENFORCEMENT, INTERNAL REVENUE SERVICE; SUE ARMSTRONG, ACTING DEPUTY ASSISTANT SECRETARY, OFFICE OF INFRASTRUCTURE PROTECTION AND GARY SCHENKEL, DIRECTOR, FEDERAL PROTECTIVE SERVICE, NATIONAL PROTECTION AND PROGRAMS DIRECTORATE, U.S. DEPARTMENT OF HOMELAND SECURITY; AND GUY COTTRELL, DEPUTY CHIEF POSTAL INSPECTOR, U.S. POSTAL INSPECTION SERVICE

STATEMENT OF MARK GOLDSTEIN

Mr. GOLDSTEIN. Good afternoon, and thank you for the opportunity to discuss GAO's recent work on the Federal Protective Service and its efforts to protect Federal facilities. Recent events, including last month's attack on Internal Revenue Service offices in Texas and the January 2010 shooting in the lobby of a Nevada Federal courthouse demonstrate the continued vulnerability of Federal facilities and the safety of Federal employees who occupy them. These events also highlight the continued challenges involved in protecting Federal real property and reiterate the importance of the Protective Service's efforts to protect the over 1 million Government employees and members of the public who work in and visit the nearly 9,000 Federal facilities.

This testimony is based on past GAO reports and testimonies and discusses challenges FPS faces in protecting Federal facilities and tenant agencies' perspectives of FPS's services. To perform this work, GAO visited a number of Federal facilities, surveyed tenant agencies, analyzed documents, interviewed officials from Federal agencies and contract guard companies.

Over the past 5 years, we have reported that FPS faces a number of operational challenges protecting Federal facilities, including the following: First, FPS' ability to manage risk across Federal facilities and implement security countermeasures is limited. FPS assesses risk and recommends countermeasures to the General Services Administration and their tenant agencies; however, decisions to implement these countermeasures are frequently made by GSA and tenant agencies who have, at times, been unwilling to fund the countermeasures.

Additionally, FPS takes a building-by-building approach to risk management, rather than taking a more comprehensive strategic approach in assessing risks among all buildings in GSA's inventory

and recommending countermeasure priorities to GSA and tenant agencies.

Second, FPS has experienced difficulty ensuring that it has a sufficient staff, and its inspector-based work force approach raises questions about protection of Federal facilities.

While FPS is currently operating at its congressionally mandated staffing level of no fewer than 1,200 full-time employees, the agency has experienced difficulty determining its optimal staffing level to protect Federal facilities. Additionally, until recently FPS' staff was steadily declining, and as a result critical law enforcement services have been reduced or eliminated.

Third, FPS does not fully ensure that its contract security guards have the training and certifications required to be deployed to a Federal facility. We found that FPS guards had not received adequate training to conduct their responsibilities. Specifically, some guards were not provided building-specific training, such as what actions to take during a building emergency or evacuation. This lack of training may have contributed to several incidents where guards neglected assigned responsibilities.

Fourth, GSA has not been satisfied with FPS' performance, and some tenant agencies are unclear on FPS' role in protecting Federal facilities. According to GSA, FPS has not been responsive and timely in providing security assessments for new leases. About one-third of FPS' customers could not comment on FPS' level of communication on various topics, including security assessments, a response that suggests a division of roles and responsibilities between FPS and its customer is unclear. Some 82 percent did not use FPS for primary law enforcement response.

FPS is taking steps to better protect Federal facilities. For example, FPS is developing a new risk assessment program and it has recently focused on improving oversight of its contract guard program.

While GAO is not making any new recommendations in this testimony, we note that FPS has not completed many related corrective actions to our previous reports. We look forward to continued progress from DHS in the near future.

Mr. Chairman, this concludes my statement. I would be happy to answer questions you and the subcommittee may have. Thank you.

[The prepared statement of Mr. Goldstein follows:]

United States Government Accountability Office

GAO

Testimony

Before the Subcommittee on Federal Workforce, Postal Service and the District of Columbia, Committee on Oversight and Government Reform, House of Representatives

For Release on Delivery
Expected at 2:00 p.m. EDT
Tuesday, March 16, 2010

HOMELAND SECURITY

Ongoing Challenges Impact the Federal Protective Service's Ability to Protect Federal Facilities

Statement of Mark L. Goldstein, Director
Physical Infrastructure Issues

GAO-10-506T

GAO
Accountability·Integrity·Reliability

Highlights

Highlights of GAO-10-506T, a testimony before the Subcommittee on Federal Workforce, Postal Service and the District of Columbia, Committee on Oversight and Government Reform, House of Representatives

Why GAO Did This Study

Recent events including last month's attack on Internal Revenue Service offices in Texas, and the January 2010 shooting in the lobby of the Nevada federal courthouse demonstrate the continued vulnerability of federal facilities and the safety of the federal employees who occupy them. These events also highlight the continued challenges involved in protecting federal real property and reiterate the importance of protecting the over 1 million government employees, as well as members of the public, who work in and visit the nearly 9,000 federal facilities.

This testimony is based on past GAO reports and testimonies and discusses challenges Federal Protective Service (FPS) faces in protecting federal facilities and tenant agencies' perspective of FPS's services. To perform this work, GAO visited a number of federal facilities, surveyed tenant agencies, analyzed documents, and interviewed officials from several federal agencies.

What GAO Recommends

GAO makes no new recommendations in this testimony. DHS concurred with GAO's past recommendations for FPS, but FPS has not completed many related corrective actions.

View GAO-10-506T or key components. For more information, contact Mark L. Goldstein at (202) 512-2834 or goldsteinm@gao.gov.

March 16, 2010

HOMELAND SECURITY

Ongoing Challenges Impact the Federal Protective Service's Ability to Protect Federal Facilities

What GAO Found

Over the past 5 years GAO has reported that FPS faces a number of operational challenges protecting federal facilities, including:

- *FPS's ability to manage risk across federal facilities and implement security countermeasures is limited.* FPS assesses risk and recommends countermeasures to the General Services Administration (GSA) and its tenant agencies, however decisions to implement these countermeasures are the responsibility of GSA and tenant agencies who have at times been unwilling to fund the countermeasures. Additionally, FPS takes a building-by-building approach to risk management, rather than taking a more comprehensive, strategic approach and assessing risks among all buildings in GSA's inventory and recommending countermeasure priorities to GSA and tenant agencies.

- *FPS has experienced difficulty ensuring that it has sufficient staff and its inspector-based workforce approach raises questions about protection of federal facilities.* While FPS is currently operating at its congressionally mandated staffing level of no fewer than 1,200 full-time employees, FPS has experienced difficulty determining its optimal staffing level to protect federal facilities. Additionally, until recently FPS's staff was steadily declining and as a result critical law enforcement services have been reduced or eliminated.

- *FPS does not fully ensure that its contract security guards have the training and certifications required to be deployed to a federal facility.* GAO found that FPS guards had not received adequate training to conduct their responsibilities. Specifically, some guards were not provided building-specific training, such as what actions to take during a building evacuation or a building emergency. This lack of training may have contributed to several incidents where guards neglected their assigned responsibilities.

GSA has not been satisfied with FPS's performance, and some tenant agencies are unclear on FPS's role in protecting federal facilities. According to GSA, FPS has not been responsive and timely in providing security assessments for new leases. About one-third of FPS's customers could not comment on FPS's level of communication on various topics including security assessments, a response that suggests that the division of roles and responsibilities between FPS and its customers is unclear.

FPS is taking some steps to better protect federal facilities. For example, FPS is developing a new risk assessment program and has recently focused on improving oversight of its contract guard program.

Mr. Chairman and Members of the Subcommittee:

We are pleased to be here to discuss the challenges the Federal Protective Service (FPS) faces and tenant agencies' perspective of the services FPS provides in protecting more than 1 million government employees, as well as members of the public, who work in and visit the nearly 9,000 federal facilities that are under the control and custody of the General Services Administration (GSA). While there has not been a large-scale terrorist attack on a domestic federal facility since the terrorist attacks of September 11, 2001, and the 1995 bombing of the Alfred P. Murrah Federal Building in Oklahoma City, recent events including last month's attack on Internal Revenue Service offices in Austin, Texas, and the January 2010 shooting in the lobby of the Las Vegas, Nevada, federal courthouse demonstrate the continued vulnerability of federal facilities and the need to ensure the safety of the federal employees who occupy them. These recent events also continue to demonstrate the challenges involved in protecting federal real property and are part of the reason GAO has designated federal real property management as a high-risk area.[1]

FPS—located within the National Protection and Programs Directorate (NPPD) of the Department of Homeland Security (DHS)—is responsible for protecting the buildings, grounds, and property that are under the control and custody of GSA, as well as the persons on that property; authorized to enforce federal laws and regulations aimed at protecting GSA buildings and persons on the property; and authorized to investigate offenses against these buildings and persons.[2] FPS conducts its mission by providing security services through two types of activities: (1) physical security activities, including conducting risk assessments of facilities and recommending countermeasures, aimed at preventing incidents at facilities and (2) law enforcement activities, including proactively patrolling facilities, responding to incidents, conducting criminal investigations, and exercising arrest authority. To accomplish its mission, FPS currently has a budget of around $1 billion, about 1,225 full-time employees, and about 15,000 contract guards deployed at federal facilities across the country.

[1]GAO, *High-Risk Series: An Update*, GAO-09-271 (Washington, D.C.: Jan. 22, 2009).

[2]40 U.S.C § 1315.

This testimony is based on our past reports and testimonies[3] and discusses challenges FPS faces in protecting federal facilities, as well as GSA and tenant agencies' views on the services FPS's provides.[4] Work for these past reports and testimonies included assessing FPS's facility protection efforts using our key security practices as a framework. We also visited FPS regions and selected GSA buildings to assess FPS activities firsthand. We surveyed a generalizable sample of 1,398 federal officials who work in GSA buildings in FPS's 11 regions and are responsible for collaborating with FPS on security issues. Additionally, we reviewed training and certification data for 663 randomly selected guards in 6 of FPS's 11 regions. Because of the sensitivity of some of the information in our prior work, we cannot specifically identify in this testimony the locations of the incidents discussed. For all of our work, we reviewed related laws and directives; interviewed officials and analyzed documents and data from DHS and GSA; and interviewed tenant agency representatives, contactors, and guards. These reviews took place between April 2007 and September 2009. The previous work on 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.

[3]This testimony draws upon six primary sources. We reported on FPS's allocation of resources using risk management, leveraging of technology, and information sharing and coordination in GAO, *Homeland Security: Greater Attention to Key Practices Would Improve the Federal Protective Service's Approach to Facility Protection*, GAO-10-142 (Washington, D.C.: Oct. 23, 2009), and GAO, *Homeland Security: Greater Attention to Key Practices Would Help Address Security Vulnerabilities at Federal Buildings*, GAO-10-236T (Washington, D.C.: Nov. 18, 2009). We reported on FPS's strategic management of human capital in 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); GAO, *Homeland Security: Preliminary Results Show Federal Protective Service's Ability to Protect Federal Facilities Is Hampered By Weaknesses in Its Contract Security Guard Program*, GAO-09-859T (Washington, D.C.: July 8, 2009); and GAO, *Homeland Security: Federal Protective Service Should Improve Human Capital Planning and Better Communicate with Tenants*, GAO-09-749 (Washington, D.C.: July 30, 2009). We reported on FPS's performance measurement and testing in 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).

[4]Tenant agencies are also referred to as FPS's customers.

FPS Faces Challenges in Protecting Federal Facilities

FPS's Ability to Manage Risk Across Facilities and Implement Security Countermeasures Is Limited

FPS assesses risk and recommends countermeasures to GSA and tenant agencies; however, FPS's ability to use risk management to influence the allocation of resources is limited because resource allocation decisions are the responsibility of GSA and tenant agencies—in the form of Facility Security Committees (FSC)—who have at times been unwilling to fund the countermeasures FPS recommends. We have found that, under the current risk management approach, the security equipment that FPS recommends and is responsible for acquiring, installing, and maintaining may not be implemented for several reasons including the following:

- tenant agencies may not have the security expertise needed to make risk-based decisions,
- tenant agencies may find the associated costs prohibitive,
- the timing of the assessment process may be inconsistent with tenant agencies' budget cycles,
- consensus may be difficult to build amount multiple tenant agencies, or
- tenant agencies may lack a complete understanding of why recommended countermeasures are necessary because they do not receive security assessments in their entirety.[5]

For example, in August 2007, FPS recommended a security equipment countermeasure—the upgrade of a surveillance system shared by two high-security locations that, according to FPS officials, would cost around $650,000. While members of one FSC told us they approved spending between $350,000 and $375,000 to fund their agencies' share of the countermeasure, they said that the FSC of the other location would not

[5]Historically, FPS has not shared its security assessments with GSA or tenant agencies, but it instead provided an executive summary. However, in his November 2009 testimony, FPS's Director stated this will change with the implementation of FPS's new security assessment tool, Risk Assessment and Management Program (RAMP), and that the security assessment would be fully disclosed and shared with GSA.

approve funding; therefore, FPS could not upgrade the system as it had recommended. In November 2008, FPS officials told us that they were moving ahead with the project by drawing on unexpended revenues from the two locations' building-specific fees as well as the funding that was approved by one of the FSCs. Furthermore, FPS officials, in May 2009, told us that all cameras had been repaired, and all monitoring and recording devices had been replaced, and that the two FSCs had approved additional upgrades, which FPS was implementing. As we reported in June 2008, we have found other instances in which recommended security countermeasures were not implemented at some of the buildings we visited because FSC members could not agree on which countermeasures to implement or were unable to obtain funding from their agencies. Currently no guidelines exist outlining the requirements for FSCs including their composition, requirements, and relationship with FPS. The Interagency Security Committee (ISC), which is chaired within NPPD, recently began to develop guidance for FSC operations, which may address some of these issues. The ISC, however, has yet to announce an anticipated date for issuance of this guidance.

Compounding this situation, FPS takes a building-by-building approach to risk management, using an outdated risk assessment tool to create facility security assessments (FSA), rather than taking a more comprehensive, strategic approach and assessing risks among all buildings in GSA's inventory and recommending countermeasure priorities to GSA and tenant agencies. As a result, the current approach provides less assurance that the most critical risks at federal buildings across the country are being prioritized and mitigated. Also, GSA and tenant agencies have concerns about the quality and timeliness of FPS's risk assessment services and are taking steps to obtain their own risk assessments. For example, GSA officials told us they have had difficulties receiving timely risk assessments from FPS for space GSA is considering leasing. These risk assessments must be completed before GSA can take possession of the property and lease it to tenant agencies. An inefficient risk assessment process for new lease projects can add to costs for GSA and create problems for both GSA and tenant agencies that have been planning for a move. Therefore, GSA is updating a risk assessment tool that it began developing in 1998, but has not recently used, to better ensure the timeliness and comprehensiveness of these risk assessments. GSA officials told us that, in the future, they may use this tool for other physical security activities, such as conducting other types of risk assessments and determining security countermeasures for new facilities. Additionally, although tenant agencies have typically taken responsibility for assessing risk and securing the interior of their buildings, assessing exterior risks

requires additional expertise and resources. This is an inefficient approach considering that tenant agencies are paying FPS to assess building security.

FPS Has Experienced Difficulty Ensuring That It Has Sufficient Staff, and Its Inspector-Based Workforce Approach Raises Questions About Protection of Federal Facilities

While FPS is currently operating at its congressionally mandated staffing level of no fewer than 1,200 full-time employees, FPS has experienced difficulty determining its optimal staffing level to protect federal facilities.[6] Prior to this mandate, FPS's staff was steadily declining and, as a result, critical law enforcement services have been reduced or eliminated. For example, FPS has largely eliminated its use of proactive patrol to prevent or detect criminal violations at many GSA buildings. According to some FPS officials at regions we visited, not providing proactive patrol has limited its law enforcement personnel to a reactive force. Additionally, officials stated that, in the past, proactive patrol permitted its police officers and inspectors to identify and apprehend individuals that were surveilling GSA buildings. In contrast, when FPS is not able to patrol federal buildings, there is increased potential for illegal entry and other criminal activity. In one city we visited, a deceased individual had been found in a vacant GSA facility that was not regularly patrolled by FPS. FPS officials stated that the deceased individual had been inside the building for approximately 3 months.

In addition to the elimination of proactive patrol, many FPS regions have reduced their hours of operation for providing law enforcement services in multiple locations, which has resulted in a lack of coverage when most federal employees are either entering or leaving federal buildings or on weekends when some facilities remain open to the public. Moreover, some FPS police officers and inspectors also said that reducing hours has increased their response times in some locations by as much as a few hours to a couple of days, depending on the location of the incident. The decrease in FPS's duty hours has also jeopardized police officer and inspector safety, as well as building security. Some inspectors said that they are frequently in dangerous situations without any FPS backup because many regions have reduced their hours of operations and overtime.

[6]This mandate has been included in FPS's annual appropriations acts for fiscal years 2008, 2009, and 2010. Appropriations are presumed to be annual appropriations and applicable to the fiscal year unless specified to the contrary. See Pub. L. No. 110-161, Division E, 121 Stat. 1844, 2051-2052 (2007); Pub. L. No. 110-329, Division D, 122 Stat. 3574, 3659-3660 (2008); and Pub. L. No. 111-83, 123 Stat. 2142, 2156-2157 (2009).

In 2008, FPS transitioned to an inspector-based workforce—eliminating the police officer position—and is relying primarily on FPS inspectors for both law enforcement and physical security activities, which has hampered its ability to protect federal facilities.[7] FPS believes that an inspector-based workforce approach ensures that its staff has the right mix of technical skills and training needed to accomplish its mission. However, FPS's ability to provide law enforcement services under its inspector-based workforce approach may be diminished because FPS relies on its inspectors to provide both law enforcement and physical security services simultaneously. This approach has contributed to a number of issues. For example, FPS faces difficulty ensuring the quality and timeliness of FSAs and adequate oversight of its 15,000 contract security guards. In addition, in our 2008 report, we found that representatives of several local law enforcement agencies we visited were unaware of FPS's transition to an inspector-based workforce and stated that their agencies did not have the capacity to take on the additional job of responding to incidents at federal facilities. In April 2007, a DHS official and several FPS inspectors testified before Congress that FPS's inspector-based workforce approach requires increased reliance on state and local law enforcement agencies for assistance with crime and other incidents at GSA facilities and that FPS would seek to enter into memorandums of agreement (MOA) with local law enforcement agencies. However, according to FPS's Director, the agency decided not to pursue MOA with local law enforcement officials, in part because of reluctance on the part of local law enforcement officials to sign such MOAs. In addition, FPS believes that the MOAs are not necessary because 96 percent of the properties in its inventory are listed as concurrent jurisdiction facilities where both federal and state governments have jurisdiction over the property.[8] Nevertheless, these MOAs would clarify roles and responsibilities of local law enforcement agencies when responding to crime or other incidents.

[7]This model was intended to make more efficient use of FPS's declining staffing levels by increasing focus on FPS's physical security duties and consolidating law enforcement activities. FPS's goal was to shift its law enforcement workforce composition from a mix of about 40 percent police officers, about 50 percent inspectors, and about 10 percent special agents, to a workforce primarily composed of inspectors and some special agents.

[8]Under the Assimilative Crimes Act, state law may be assimilated to fill gaps in federal criminal law where the federal government has concurrent jurisdiction with the state. 18 U.S.C. §13.

Insufficient Oversight and Inadequate Training of Contract Guards Has Hampered FPS's Protection of Federal Facilities

FPS does not fully ensure that its contract security guards have the training and certifications required to be deployed to a GSA building. FPS maintains a contract security guard force of about 15,000 guards that are primarily responsible for controlling access to federal facilities by (1) checking the identification of government employees, as well as members of the public who work in and visit federal facilities and (2) operating security equipment, including X-ray machines and magnetometers, to screen for prohibited materials such as firearms, knives, explosives, or items intended to be used to fabricate an explosive or incendiary device. We reported in July 2009, that 411 of the 663 guards (62 percent) employed by seven FPS contractors and deployed to federal facilities had at least one expired certification, including a declaration that the guards have not been convicted of domestic violence, which makes them ineligible to carry firearms.

We also reported in July 2009, that FPS guards had not received adequate training to conduct their responsibilities. FPS requires that all prospective guards complete about 128 hours of training including 16 hours of X-ray and magnetometer training. However, in one region, FPS has not provided the X-ray or magnetometer training to its 1,500 guards since 2004. Nonetheless, these guards are assigned to posts at GSA buildings. X-ray training is critical because guards control access points at buildings. In addition, we also found that some guards were not provided building-specific training, such as what actions to take during a building evacuation or a building emergency. This lack of training may have contributed to several incidents where guards neglected their assigned responsibilities. Following are some examples:

- at a level IV facility,[9] the guards did not follow evacuation procedures and left two access points unattended, thereby leaving the facility vulnerable;

[9]The level of security FPS provides at each of the 9,000 federal facilities varies depending on the building's security level. Based on the Department of Justice's (DOJ) 1985 "Vulnerability Assessment Guidelines," there are five types of security levels. A level I facility is typically a small storefront-type operation such as military recruiting office that has 10 or fewer employees and a low volume of public contact. A level II facility has from 11 to 150 employees, a level III facility has from 151 to 450 employees and moderate to high volume of public contact, a level IV facility has over 450 employees, a high volume of public contact, and includes high-risk law enforcement and intelligence agencies. FPS does not have responsibility for level V facilities which include the White House and the Central Intelligence Agency. The ISC has recently promulgated new security level standards that will supersede the 1995 DOJ standards.

- at a level IV facility, the guard allowed employees to enter the building while an incident involving suspicious packages was being investigated; and
- at a level III facility, the guard allowed employees to access the area affected by a suspicious package; this area was required to be evacuated.

We also found that FPS has limited assurance that its guards are complying with post orders.[10] In July 2009, we reported that FPS does not have specific national guidance on when and how guard inspections should be performed. Consequently, inspections of guard posts in 6 of the 11 regions we visited were inconsistent and varied in quality. We also found that guard inspections in the 6 regions we visited are typically completed by FPS during regular business hours and in locations where FPS has a field office and seldom at nights or on weekends or in nonmetropolitan areas. For example, in 2008, tenants in a level IV federal facility in a nonmetropolitan area complained to a GSA property manager that they had not seen FPS in over 2 years, there was no management of their guards, and the number of incidents at their facility was increasing. GSA officials contacted FPS officials and requested FPS to send inspectors to the facility to address the problems. Most guards are also stationed at fixed posts that they are not permitted to leave, which can impact their response to incidents. For example, we interviewed over 50 guards and asked them whether they would assist an FPS inspector chasing an individual in handcuffs escaping a federal facility. The guards' responses varied, and some guards stated they would likely do nothing and stay at their posts because they feared being fired for leaving. Other guards also told us that they would not intervene because of the threat of a liability suit for use of force and did not want to risk losing their jobs. Additionally, guards do not have arrest authority, although contract guards do have authority to detain individuals. However, according to some regional officials, contract guards do not exercise their detention authority also because of liability concerns.

[10]At each guard post, FPS maintains a book, referred to as post orders, that describes the duties that guards are to perform while on duty.

GSA Has Not Been Satisfied With FPS's Performance and Some Tenant Agencies Are Unclear On FPS's Role In Protecting Federal Facilities

We found that GSA—the owner and lessee of many FPS protected facilities—has not been satisfied with the level of service FPS has provided since FPS transferred to DHS. For example, according to GSA officials, FPS has not been responsive and timely in providing assessments for new leases. GSA officials in one region told us that the quality of the assessments differs depending on the individual conducting the assessment. This official added that different inspectors will conduct assessments for the same building so there is rarely consistency from year to year, and often inspectors do not seem to be able to fully explain the countermeasures that they are recommending. We believe that FPS and GSA's information sharing and coordination challenges are primarily a result of not finalizing a new MOA that formalizes their roles and responsibilities. According to GSA officials, in November 2009, the two agencies have met to start working through the MOA section by section, and as of early March 2010 they have had four working group sessions and are anticipating an initial agreed upon draft in late spring 2010. In the absence of a clearly defined and enforced MOA, FPS officials told us they feel they are limited in their ability to protect GSA properties.

Additionally, in 2009, we reported that tenant agencies have mixed views about some of the services they pay FPS to provide.[11] For example, according to our generalizable survey of tenant agencies,

- About 82 percent of FPS's customers indicated they do not use FPS as their primary law enforcement agency in emergency situations, and said they primarily rely on other agencies such as local law enforcement, the U.S. Marshals Service, or the Federal Bureau of Investigation; 18 percent rely on FPS.
- About one-third of FPS's customers indicated that they were satisfied with FPS's level of communication, one-third were neutral or dissatisfied, while the remaining one-third could not comment on how satisfied or dissatisfied they were with FPS's level of communication on various topics including building security assessments, threats to their facility, and security guidance This response that suggests that the division of roles and responsibilities between FPS and its customers is unclear.

[11]GAO-09-749.

Our survey also suggests that this lack of clarity is partly due to the little or no interaction customers have with FPS officers. Examples are as follows:

- A respondent in a leased facility commented that FPS has very limited resources, and the resources that are available are assigned to the primary federally owned building in the region.
- A respondent remembered only one visit from an FPS officer in the last 12 years.

FPS Is Taking Steps to Better Protect Federal Facilities

Over the past 5 years, we have conducted a body of work reviewing the operations of FPS and its ability to adequately protect federal facilities and we have made numerous recommendations to address these challenges. For example, we recommended FPS improve its effective long-term human capital planning, clarify roles and responsibilities of local law enforcement agencies in regard to responding to incidents at GSA facilities, develop and implement performance measures in various aspects of its operations, and improve its data collection and quality across its operations. While FPS has generally agreed with all of our recommendations, it has not completed many related corrective actions.

At the request of Congress we are in the process of evaluating some of FPS's most recent actions. For example, FPS is developing the Risk Assessment and Management Program (RAMP), which could enhance its approach to assessing risk, managing human capital, and measuring performance. With regard to improving the effectiveness of FPS's risk management approach and the quality of FSAs, FPS believes RAMP will provide inspectors with the information needed to make more informed and defensible recommendations for security countermeasures. FPS also anticipates that RAMP will allow inspectors to obtain information from one electronic source, generate reports automatically, track selected countermeasures throughout their life cycle, and address some concerns about the subjectivity inherent in FSAs.

In response to our July 2009 testimony, FPS took a number of immediate actions with respect to contract guard management. For example, the Director of FPS instructed Regional Directors to accelerate the implementation of FPS's requirement that two guard posts at Level IV facilities be inspected weekly. FPS also required more X-ray and magnetometer training for inspectors and guards.

To improve its coordination with GSA, the FPS Director and the Director of GSA's Public Buildings Service Building Security and Policy Division participate in an ISC executive steering committee, which sets the committee's priorities and agendas for ISC's quarterly meetings. Additionally, FPS and GSA have established an Executive Advisory Council to enhance the coordination and communication of security strategies, policies, guidance, and activities with tenant agencies in GSA buildings. This council could enhance communication and coordination between FPS and GSA, and provide a vehicle for FPS, GSA, and tenant agencies to work together to identify common problems and devise solutions.

We plan to provide Congress with our final reports on FPS's oversight of its contract guard program and our other ongoing FPS work later this year.

Mr. Chairman, this completes my prepared statement. I would be happy to respond to any questions you or other members of the committee may have at this time.

GAO Contact and Staff Acknowledgement

For further information on this testimony, please contact me at (202) 512-2834 or by e-mail at goldsteinm@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this statement. Individuals making key contributions to this testimony include Tammy Conquest, Assistant Director; Tida Barakat; Jonathan Carver; Delwen Jones; and Susan Michal-Smith.

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.

GAO's Mission	The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.
Obtaining Copies of GAO Reports and Testimony	The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday afternoon, GAO posts on its Web site newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to www.gao.gov and select "E-mail Updates."
Order by Phone	The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's Web site, http://www.gao.gov/ordering.htm. Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537. Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.
To Report Fraud, Waste, and Abuse in Federal Programs	Contact: Web site: www.gao.gov/fraudnet/fraudnet.htm E-mail: fraudnet@gao.gov Automated answering system: (800) 424-5454 or (202) 512-7470
Congressional Relations	Ralph Dawn, Managing Director, dawnr@gao.gov, (202) 512-4400 U.S. Government Accountability Office, 441 G Street NW, Room 7125 Washington, DC 20548
Public Affairs	Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800 U.S. Government Accountability Office, 441 G Street NW, Room 7149 Washington, DC 20548

Please Print on Recycled Paper

Mr. LYNCH. Thank you, Mr. Goldstein.

Mr. Miller, you are now recognized for 5 minutes for an opening statement.

STATEMENT OF STEVEN MILLER

Mr. MILLER. Thank you, Chairman Lynch, Ranking Member Chaffetz, and Congresswoman Norton. Thanks for the opportunity to testify on IRS workplace safety and security, particularly in the wake of the senseless attack last month on the IRS building in Austin, TX, that took the life of Vernon Hunter.

We are dedicated to ensuring safety and the well-being of our 100,000 employees, no matter what their job is nor where they are located. The IRS work force is our most valuable resource, and no violent act is going to deter us from doing our jobs with dignity and respect for the American public.

At the IRS security is managed by our Office of Physical Security and Emergency Preparedness, which manages at a national level, ensuring we have consistent implementation of security policies and procedures. For 2010, we will spend just over $100 million on security at IRS offices. There are over 700 such facilities.

As required under an Executive order, we utilize the Interagency Security Committee [ISC] standards, to determine what security to provide at a given facility. Depending upon the applicable security level under the standards, we will provide a variety of security tools, including highly visible guards and K–9s, explosive and intrusion detection systems.

We also employ access control systems such as turnstiles, card key access, proximity cards, and lock and key control systems. Physical barriers include bollards, crash fencing, barriers, planters, and pop-up barriers. Screening measures focus on magnetometers, hand-held wands, and x-ray machines. We also have a detailed incident reporting system that is available and up and running 24/7, 365 days of the year that reports and tracks on these incidents.

Mr. Chairman, the IRS employs a combination of strategies to plan, implement, and evaluate our security processes, and we promote security and awareness for all IRS employees. Our employees, in fact, are our partners in ensuring security, workplace safety and security.

In this regard, we conduct periodic evacuation drills and shelter and place exercises which heighten employee emergency readiness. If you watched any of the coverage in Austin, you saw that among the things that went right down there—and some things did, in fact, go right, Mr. Chairman—our drills proved their worth. People did get out of the building on a timely basis and we lost only one life.

We also issue recurring communications regarding security and safety to reinforce processes and to raise awareness, including annual security awareness fairs that are held across the country, and we maintain an IRS internet Web site that provides updated information on IRS physical security and emergency preparedness programs.

From what I know today, Mr. Chairman, it is unlikely that there is anything we could have done to prevent the attack in Austin. Nonetheless, following that attack we took a series of immediate

steps to enhance our security posture both in Austin and across the country while we assess our long-term security needs and whether they have changed over time. This increased vigilance includes 24/7 guard service in all 11 IRS Austin offices. There is also additional security at IRS facilities across the country, including additional guard service at this time.

In conclusion, this area remains a top concern for the IRS, and we will be taking a hard look at what we can do in both the short and long term to ensure the safety of our folks. Nothing is more important to Treasury Secretary Geithner, Commissioner Shulman, nor myself.

Thanks. I will be happy to take any questions.

[The prepared statement of Mr. Miller follows:]

PREPARED STATEMENT OF
STEVEN T. MILLER
DEPUTY COMMISSIONER FOR SERVICES AND ENFORCEMENT
INTERNAL REVENUE SERVICE
BEFORE THE
COMMITTEE ON
OVERSIGHT AND GOVERNMENT REFORM
SUBCOMMITTEE ON THE
FEDERAL WORKFORCE, POSTAL SERVICE
AND THE DISTRICT OF COLUMBIA
HEARING ON WORKPLACE SAFETY
UNITED STATES HOUSE OF REPRESENTATIVES
MARCH 16, 2010

Introduction

Chairman Lynch, Ranking Member Chaffetz, Members of the Subcommittee, thank you for this opportunity to testify on IRS workplace safety and security, particularly in the wake of the senseless and horrific attack last month upon the IRS Austin Echelon facility that took the life of one of our employees – Mr. Vernon Hunter.

Commissioner Shulman and his entire senior leadership team are dedicated to ensuring the safety and well being of our 100,000 employees, no matter what their job or where their post of duty may be. The IRS workforce is our most valuable resource. And as the Commissioner told our Austin employees, this violent act will not deter us from doing our jobs with dignity and respect for all Americans.

Overview

IRS Security is managed by Physical Security and Emergency Preparedness (PSEP), which has a national scope, thereby ensuring consistent implementation of security policies and procedures across the entire IRS enterprise. The cost to provide security at IRS offices for fiscal year 2010 is just over $100 million.

There are over 700 IRS facilities, of which the overwhelming majority are occupied by IRS employees; the remaining are parking structures, child care centers, credit unions, storage, and warehouse facilities.

Methodology

As required by Executive Order 12977 (signed October 19, 1995), IRS utilizes the Interagency Security Committee (ISC) standards as the baseline for providing security for IRS personnel, assets, and sensitive taxpayer information.

There are many advantages to this approach. For example, ISC standards provide for a consistent approach to providing security throughout the United States Government and these are the established standards.

I would also like to share with the Subcommittee some greater detail on the various security methods we employ depending on the applicable security level dictated under the ISC standards. For example, highly visible guards and canines engage in patrols, search and explosive detection. Intrusion detection systems include alarms, glass breaks and motion detectors.

We also employ access control systems, such as turnstiles, card key access (proximity cards) and lock and key control systems. Physical barriers include: bollards, crash-related fencing/barriers/planters and pop-up barriers.

Screening measures focus on magnetometers, hand-held wands and X-Ray machines. We also have incident reporting/Situational Awareness Management Centers to provide 24/7/365 reporting of incidents.

Security Process Programs and Efforts to Prepare Employees for Emergency Situations

Mr. Chairman, the IRS also employs a combination of strategies to plan, implement and evaluate our security processes. These include:

- Occupant Emergency Plans
- Business Resumption / Continuity Plans
- Information Management Plan
- Disaster Recovery/Information Technology Contingency Plan

In addition, we promote security and awareness to all IRS employees. They are our partners when it comes to workplace safety and security.

We conduct evacuation drills and shelter-in-place exercises which heighten employee emergency readiness. They proved their worth in Austin.

We also issue recurring communications regarding security and safety protocols and processes to re-enforce their importance and raise awareness. To this end, we also maintain an IRS Intranet website that provides updated information on IRS' physical security and emergency preparedness programs.

In addition, the IRS conducts an annual Security Awareness Fair where we make available to employees information on security and emergency preparedness programs.

Security Enhancements – Post Austin

Following the attack upon the Austin Echelon building, we took a series of immediate steps to enhance our security posture both in Austin and across the country while we assess our long-term security needs. The increased vigilance at the Austin Office includes continuing to check the identification of persons entering offices, conducting random searches, and overall guard presence and visibility. There is now 24/7 guard service in all eleven IRS Austin offices.

There is also additional security at IRS facilities across the country including additional guard service. And the Federal Protection Service initialized Operational Shield to conduct verifications of official identification, screen vehicles for explosives and conduct interior patrolling and patrols of the exterior grounds and facility perimeters.

Conclusion

In conclusion, this area remains a top concern for the IRS, and we will be taking a hard look at what we can do in both the short- and long-term to ensure the safety of our employees. Nothing is more important to Treasury Secretary Geithner, the Commissioner, or me. Thank you and I would be happy answer your questions.

Mr. LYNCH. Thank you, Mr. Miller.

Ms. Armstrong, you are now welcome to offer testimony for 5 minutes.

STATEMENT OF SUE ARMSTRONG

Ms. ARMSTRONG. Thank you, Chairman Lynch, Ranking Member Chaffetz, and Congresswoman. It is a pleasure to appear before you today to discuss the work of the Interagency Security Committee. The Interagency Security Committee was created as a direct result of the Oklahoma City bombing of the Alfred P. Murrah Federal Building in 1995, the worst domestic-based terrorist attack in U.S. history.

The mission of the Interagency Security Committee is to develop standards, policies, and best practices for enhancing the quality and effectiveness of physical security in and the protection of the over 300,000 non-military Federal facilities in the United States. The Department of Homeland Security's Assistant Secretary for Infrastructure Protection chairs the Interagency Security Committee, which is composed of senior executives from 45 member departments and agencies that contribute to the publication of innovative products to increase the security of Federal facilities, to protect Federal employees and the visiting public.

For example, in March 2008 the Interagency Security Committee developed and published the facility security level determinations for Federal facilities, which defines criteria and processes facilities should use to determine their facilities security level. In June 2009, per recommendation from the Government Accountability Office, the Interagency Security Committee developed the use of physical security performance measures, the first Federal policy guidance on performance measures for physical security programs and testing procedures.

In addition, the Interagency Security Committee is currently in the final stages of a comprehensive, multi-year effort to integrate 15 years of standards, lessons learned, and countermeasures for threats to federally owned and leased facilities. These documents will comprise the most comprehensive standards for Federal facilities created to date.

The Assistant Secretary for Infrastructure Protection also oversees the work of the Office of Infrastructure Protection, which conducts vulnerability assessments on the Government facilities sector. These assessments identify security gaps and provide the foundation for risk-based implementation of protective programs. The Office of Infrastructure Protection also distributes the infrastructure protection report series, which provides protection information tailored to address issues faced by Federal buildings such as large Government office buildings and Federal courthouses, and my colleague from the Federal Protective Service will describe the department's role in protecting these facilities in greater detail.

I appreciate the opportunity to address the committee on this important issue and I look forward to answering any questions you might have.

Mr. LYNCH. Thank you.

Mr. Schenkel, you are welcome to offer testimony for 5 minutes.

STATEMENT OF GARY SCHENKEL

Mr. SCHENKEL. Thank you, Chairman Lynch, Ranking Member Chaffetz, Congresswoman Norton. It is a pleasure to appear before you today to discuss the actions of the Federal Protective Service as the Federal Protective Service undertakes to ensure the safety and security of Federal Government buildings.

The Federal Protective Service performs fixed post access control screening functions, roving patrols at 9,000 General Services Administration owned and leased facilities. In fiscal year 2009 the Federal Protective Service responded to 35,812 calls for service, including 1,242 protests and organized disturbances, made 1,646 arrests, conducted 1,115 criminal investigations, processed 272 weapons violations, and prevented the introduction of 661,724 prohibited items into Federal facilities, all with the significant assistance of our contract guards known as protective security officers.

FPS was transferred at the start of the fiscal year to the National Protection and Programs Directorate, a component within DHS whose core mission is national resiliency that ranges from physical infrastructure protection to cybersecurity. While we are focused on ensuring a smooth transition of the organization, we believe this new structure will better position us within the department to receive the necessary support and meet our critical responsibilities moving forward.

Primary among the Federal Protective Service's core mission requirements is the facility security assessment. The facility security assessment identifies existing and potential threats to Federal facilities and their occupants. The Federal Protective Service takes an all-hazards approach to facilities security assessment and evaluates the risk against possible mitigation measures built into our new risk assessment and management program. Those mitigating countermeasures are then presented to each facility's security committee, with recommendations on which countermeasures should be implemented, including the development of an occupant emergency plan.

The Federal Protective Service systematically measures the effectiveness of our countermeasures through a variety of systematic progress, such as annual countermeasure effectiveness inventories, scheduled guard post and guard vendor inspections, and one of our most visible means, Operation Shield.

Operation Shield conducts unannounced inspections to measure the effectiveness of contract guards in detecting the presence of unauthorized persons, potentially disruptive or dangerous activities in or around Federal facilities, and the guards' ability to prevent the introduction of prohibitive items or harmful substances into those facilities.

Operation Shield also serves as a visible, proactive, and random measure that may be used as a deterrent to disrupt the planning of terrorist activities.

In addition, the Federal Protective Service routinely provides security awareness training for employees which includes presentations on how to avoid becoming a victim of theft or violence, and we have also developed active shooter training, explaining what employees should do when faced with a violent situation and how to respond when law enforcement arrives.

FPS has taken several actions and initiatives to address major areas identified by the Government Accountability Office, including human capital management, finance, guard contract oversight. FPS continues to develop additional information collection and analysis tools.

FPS addressed the current GAO report regarding contract guard oversight and lapses in screening procedures by determining the cause of the lapses and recommending measures to prevent reoccurrence: increasing the frequency of guard posts and performance of protection security officers formerly referred to as contract security officers; requiring additional training in magnetometer and x-ray, including contract modification requiring the viewing of an FPS-produced training video that addresses screening for improvised explosive devices; ensuring that all protective security officers are compliant with certifications and qualifications, as stated in contract, by incorporating the certification system into our risk assessment management program or RAMP; developing and initiating a 16-hour magnetometer x-ray training program provided to protective security officers by Federal Protective Service inspectors titled the National Weapons Detection Program, which has begun in January 2010.

As a result of the covert testing working group, FPS developed covert testing program which enhanced and complemented the ongoing efforts to improve oversight and improve the attentiveness and professionalism of the protective security officer. This current program further achieves FPS' strategic goals of effectively and efficiently securing Federal facilities and keeping their occupants safe.

These are just some of the many ways the Federal Protective Service contributes to the safety and security of Federal buildings and their occupants.

I look forward to the opportunity to answer any questions you may have, and I thank you and the committee for holding this important hearing.

[The prepared statement of Ms. Armstrong and Mr. Schenkel follows:]

Statement for the Record
of
Sue Armstrong
Acting Deputy Assistant Secretary
Office of Infrastructure Protection
National Protection and Programs Directorate
and
Gary Schenkel
Director
Federal Protective Service
National Protection and Programs Directorate
Department of Homeland Security

Before the
United States House of Representatives
House Oversight and Government Reform Committee
Subcommittee on Federal Workforce, Postal Service, and the District of Columbia
Washington, DC

March 16, 2010

Thank you, Chairman Lynch, Ranking Member Chaffetz, and distinguished Members of the Committee. It is a pleasure to appear before you today to discuss the actions the Department of Homeland Security (DHS) has undertaken to ensure the safety and security of federal government buildings.

The Office of Infrastructure Protection (IP) and the Federal Protective Service (FPS) are both part of the National Protection and Programs Directorate (NPPD) in DHS. Part of the missions that both offices execute stem from Homeland Security Presidential Directive 7 (HSPD-7): Critical Infrastructure Identification, Prioritization, and Protection, which created a common policy and framework for the protection of the nation's critical infrastructure and key resources. Under HSPD-7, and the National Infrastructure Protection Plan that resulted from it, IP leads the coordinated national effort to reduce risk to our critical infrastructure and key resources posed by acts of terrorism and enables national preparedness, timely response, and rapid recovery in the event of an attack, natural disaster, or other emergency. FPS serves as the sector-specific agency for the Government Facilities Sector. In this role, FPS works closely with IP, the Interagency Security Committee (ISC) – chaired by the DHS Assistant Secretary for Infrastructure Protection

(IP) – and other federal, state, local, tribal, and territorial governments to coordinate risk management efforts for all government facilities to ensure that the critical missions they perform can be carried out without interruption.

We are here to discuss the distinct but related roles of FPS and the ISC in working to ensure the security and safety of employees in federal facilities. The ISC develops security standards, policies, and best practices for federal agencies responsible for protecting non-military federal facilities in the United States. One of the 45 member agencies of the ISC, the FPS provides integrated law enforcement and physical security services to federal agencies in General Services Administration (GSA)-owned and leased facilities throughout the United States and its territories. Of the 300,000 facilities covered under the ISC's standards, policies, and practices, 9,000 are protected by FPS.

ISC Background

The mandate of the ISC is to develop standards, policies, and best practices for enhancing the quality and effectiveness of physical security in, and the protection of, non-military federal facilities in the United States, and its mission is to ensure that the Federal Government safeguards U.S. civilian facilities from all hazards by developing state-of-the-art security standards in collaboration with public and private homeland security partners, including federal Chief Security Officers and other senior executives responsible for protecting non-military federal facilities across the United States.

The ISC was created as a direct result of the Oklahoma City bombing of the Alfred P. Murrah Federal Building on April 19, 1995—the deadliest attack on U.S. soil before September 11, 2001, and the worst domestic-based terrorist attack in U.S. history.

The day after the attack, President Clinton directed the Department of Justice (DOJ) to assess the vulnerability of federal facilities to acts of terrorism or violence, and to develop recommendations for minimum security standards. At that time, there were no minimum physical security standards for non-military federally owned or leased facilities.

Within 60 days of the attack, DOJ published its findings and recommendations in a landmark report, *Vulnerability Assessment of Federal Facilities*. One of the recommendations was the creation of the ISC. On Oct. 19, 1995, President Clinton issued Executive Order 12977, creating ISC to address "continuing government-wide security" for federal facilities. EO 12977 also specified the ISC membership—senior executives from 45 federal agencies and departments.

ISC Initiatives

Since the transfer of the Chair of the ISC to IP in August 2007, the ISC has published innovative products to increase security of federal facilities. In March 2008, the ISC developed and published the *Facility Security Level Determinations for Federal Facilities*, which defines criteria and processes a facility should use to determine its facility security level (FSL). The FSL is the foundation for all ISC standards. In June 2009, per a recommendation from the Government Accountability Office, the ISC developed and published the *Use of Physical Security Performance Measures* – the first federal policy guidance published about performance measures for physical security programs and testing procedures.

The ISC is currently in the final stages of a comprehensive multiyear effort that builds upon 15 years of previous interagency materials, lessons learned, and countermeasures for threats to federally owned and leased facilities. These documents comprise the most comprehensive standards for federal facilities created to date, providing consistency for all facility physical security standards.

Additional IP Federal Efforts

IP offers to conduct vulnerability assessments on the Government Facilities Sector, which includes federal buildings. Assessments include: Site Assistance Visits, Buffer Zone Plans, Computer Based Assessment Tool data (which captures critical site assets and current security postures), and Enhanced Critical Infrastructure Program/Infrastructure Survey Tool security assessments. These vulnerability assessments identify security gaps and provide the foundation

for risk-based implementation of protective programs designed to prevent, deter, and mitigate the risk of a terrorist attack while enabling timely, efficient response to an all-hazards situation.

IP also distributes the Infrastructure Protection Report Series, which includes a series of reports specifically tailored to address critical infrastructure and key resources protection issues of federal buildings, such as large government office buildings and federal courthouses. These reports, which are distributed to owners and operators who have a specific threat vector, serve to:

- Increase awareness of common facility vulnerabilities;
- Increase awareness of potential indicators of terrorist activity;
- Identify protective measures to help deter, detect, defend, respond and recover from a terrorist attack or natural/manmade disasters; and
- Build baseline security knowledge within each sector and infrastructure category.

FPS Background

FPS performs fixed-post access control, screening functions, and roving patrols of facility perimeters and communal open space at 9,000 General Services Administration (GSA)-owned and leased facilities. FPS is comprised of 1,225 federal law enforcement and support staff personnel. In order to provide physical security services to these locations, FPS utilizes the assistance of more than 15,000 contract security guards employed by private companies.

FPS Law Enforcement Security Officers, also called Inspectors, are uniformed law enforcement officers who possess the full authority and training to perform traditional police functions in connection with federal facilities. Currently, FPS has 689 Inspectors who are trained as physical security experts and provide comprehensive security services such as Facility Security Assessments and implementation and testing of security measures.

FPS and building tenants must effectively balance the need for security in federal facilities with the need for access. The public depends on the federal departments and agencies that occupy these facilities for a variety of services, and the public must have ready access to the facilities. At the same time, FPS must provide security solutions that provide a safe and secure

environment for the occupants of federal facilities. Concurrently, the security measures in place at federal facilities must not deter people from conducting regular business.

FPS Operations

FPS offers comprehensive physical security operations. From the installation of alarm systems, X-rays, magnetometers, and entry control systems, to monitoring those systems around the clock and providing uniformed police response and investigative follow-up, FPS is organized to protect and serve. The provision of contract security guard services, crime prevention seminars tailored to individual agency and employee needs, facility security surveys, integrating intelligence gathering and sharing, and maintaining special operations capabilities all comprise FPS' broad capabilities.

FPS annually conducts nearly 2,500 Facility Security Assessments and responds to approximately 1,400 demonstrations. In Fiscal Year (FY) 2009, FPS responded to 35,812 calls for service, including 1,242 protests and organized disturbances, made 1,646 arrests, conducted 1,115 criminal investigations, processed 272 weapons violations, and prevented the introduction of 661,724 prohibited items into federal facilities – all with the significant assistance of our Protective Security Officers (contract guards). Of the approximately 9,000 buildings protected by FPS, 1,500 are categorized as Security Level III or IV (highest risk buildings).

Ever since FPS was transferred from GSA in 2003 – with a Full-Time Equivalent (FTE) workforce of more than 1,400 spread across the country – to a single agency with 11 Regions with varying business practices, FPS has faced the challenge of becoming a standardized organization.

This transition required a new strategic approach to the protection mission of the FPS.
The resulting FPS Strategic Plan focused on critical issues within the protective mission and developed a sound strategic path forward focused on ensuring facilities are secure and occupants are safe.

To establish a systematic, strategic, and professional approach, FPS identified and shared best practices, developed standardized policy, identified problems and developed solutions in all financial, administrative, and operational program areas.

The FY 2008 Omnibus Appropriations Bill established a floor of 1,200 Federal FTEs for FPS, and the authority for FPS to raise fees to financially support that number. In March 2008, FPS embarked on its first hiring effort in more than six years. This monumental hiring effort was a new challenge in addition to continuing with the FPS Strategic Plan to create one consistent and standardized operation. Today, the FPS workforce is more than 1,225 FTEs strong, and growing. The strategic transformation of our workforce to acquire the appropriate skills in diverse geographic locations remains a priority and is the foundation of our comprehensive Mission Action Plan.

Although FPS does not guard the facilities involved in the recent incidents at the U.S. Holocaust Memorial Museum in Washington, D.C. or the Lloyd D. George Federal Courthouse in Las Vegas, FPS did assist in developing and exercising an Occupant Emergency Plan (OEP) for the air attack on the Internal Revenue Service (IRS) office building in Austin, Texas, the immediate implementation of which saved lives. The designated lead from each facility and the assigned FPS Inspector develop a facility-specific OEP, which includes emergency evacuation, shelter in place, and other actions determined necessary by the FSC.

Primary among FPS' varied core mission requirements is the Facility Security Assessment (FSA). The FSA is an assessment of risk on the GSA-owned or leased property that identifies existing and potential threats to federal facilities and their occupants. FPS takes an all-hazards approach to the FSA, evaluated against possible mitigation measures built into FPS's new Risk Assessment Management Program (RAMP). RAMP is a web-based system that calculates risks—including weather, geologic, terrorist, and criminal—into an equation that is then measured against countermeasures to mitigate those risks. Those mitigating countermeasures are then presented to each facility's Facility Security Committee (FSC) with recommendations on which countermeasures should be implemented, including the development of the OEP.

In addition, FPS systematically measures the effectiveness of FPS countermeasures through a program called Operation Shield. Due to their high profile, federal facilities operate in a dynamic threat environment, which requires a constant flow of reliable information about active threats to facilities and associated assets, systems, networks, and functions. Operation Shield conducts unannounced inspections to measure the effectiveness of the contract guards in detecting the presence of unauthorized persons, potentially disruptive or dangerous activities in or around federal facilities, and the guards' ability to prevent the introduction of prohibited items or harmful substances into those facilities. Operation Shield also serves as a visible, proactive, and random measure that may be used as a deterrent to disrupt the planning of terrorist activities.

FPS knows that security is not just one agency's business; it is a collective effort from many parties, including building tenants and GSA. FPS and GSA partner on countermeasure implementation, and the RAMP tool allows FPS to share the FSA with GSA efficiently. FPS also has implemented procedures to relay immediate threat information to the GSA Offices of Security.

Our greatest collective partner is the federal employee. In addition to the FSA and OEP, FPS routinely provides Security Awareness Training, which includes presentations on how to avoid becoming a victim of theft or violence. FPS has developed Active Shooter Training for employees and has already begun training at federal facilities. This training explains to employees what to do when faced with a violent situation and how to respond when law enforcement arrives.

The Protective Investigation Program (PIP) identifies individuals who may threaten or who have threatened or harmed federal employees and uses numerous and varying mitigation strategies against those who pose a threat to federal employees. This program's value lies in its ability to adapt to and address novel threats. All FPS Criminal Investigators and Special Agents are trained in the PIP.

FPS has taken several actions and initiatives to address major areas identified by the Government Accountability Office (GAO) including human capital management, finance, and contract guard

oversight. FPS refined its human capital management with the use of a strategic staff allocation model to manage its staffing resources. These accomplishments and improvements led GAO to close the recommendation that FPS develop and implement a strategic approach to manage staffing resources.

FPS employed a strategic approach to improve its business processes, and the enhancements of financial functions have paid huge dividends by improving invoice payment processes and consolidating the entire process.

FPS continues to develop additional information collection and analysis tools. FPS addressed the current GAO report regarding contract guard oversight and lapses in screening procedures by:

- Determining the causes of the lapses and recommending measures to prevent recurrence;
- Increasing the frequency of post inspections performed by Protective Security Officers (formerly referred to as contract security officers);
- Requiring additional training in magnetometer and X-ray screening including contract modification requiring the viewing of an FPS produced training video that addresses screening for improvised explosive devices;
- Ensuring that all Protective Security Officers are compliant with certifications and qualifications as stated in contract by incorporating the certification system into RAMP; and
- Developing and initiating a 16-hour magnetometer X-ray training program, provided to Protective Security Officers by FPS Inspectors, titled *National Weapons Detection Program*, which began in January 2010.

As a result of a Covert Testing Working Group, FPS developed a Covert Testing Program, which enhanced and complemented the ongoing over efforts to improve oversight and promote the attentiveness and professionalism of the Protective Security Officer. This current program further achieves FPS strategic goals of effectively and efficiently ensuring secure facilities and safe occupants.

Conclusion

The Department will continue to work with public and private homeland security partners to ensure that federal facilities are safe and secure.

Thank you for holding this important hearing. We would be happy to respond to any questions you may have.

Mr. LYNCH. Thank you, Mr. Schenkel.

Mr. Cottrell, welcome. You are now recognized for 5 minutes for an opening statement.

STATEMENT OF GUY COTTRELL

Mr. COTTRELL. Good afternoon, Chairman Lynch, Congressman Chaffetz, and Congresswoman Norton. My name is Guy Cottrell, Deputy Chief Inspector for the U.S. Postal Inspection Service. I am pleased to be here with you today to discuss safety and security practices at the Postal Service.

While I am a postal inspector, please note that in today's testimony I am providing information that reflects security strategies across many different functions within the Postal Service.

I will begin with the Inspection Service. Our mission is to protect the Postal Service and its employees, secure the Nation's mail system, and ensure public trust in the mail. Postal inspectors are Federal law enforcement officers who carry firearms, make arrests, and serve Federal search warrants and subpoenas. There are approximately 1,400 postal inspectors nationwide and abroad who enforce more than 200 Federal laws involving the use of the U.S. mail and the postal system. The Inspection Service maintains a security force staffed by roughly 650 uniformed postal police officers who are assigned to critical postal facilities across the country. The officers provide perimeter security, escort high-value mail shipments, and perform essential protective functions.

The Postal Service has a number of ways we provide security for our employees and buildings. The Postal Service has a cross-functional program to comprehensively review a building's security. Program helps postmasters and installation heads achieve and maintain compliance with policies governing all aspects of security. The review includes comprehensive onsite observations, document reviews, and interviews of facility personnel. At the conclusion of each assessment, a plan is developed to address any issues identified in that review.

Emphasizing the key role that each employee plays in each other's safety is one of our prime strategies. Special emphasis has been placed on developing employee communications safety materials. For example, each week at facilities nationwide, managers are required to give safety stand-up talks. Simple tips to employees such as reporting the condition of fences or public access to the workroom floor all contribute to employee safety.

We will shortly begin an educational campaign aimed specifically at our letter carriers.

A major component of the Postal Service's workplace violence prevention program is the district threat assessment team. Threat assessment teams use cross-functional team approaches to assess threatening situations and to develop risk abatement plans to minimize the potential risk of future violence.

The Postal Service has established an agency-wide continuity program. The continuity program deals with issues that arise prior to, during, and after an event relative outstanding the employee's safety and welfare. This program is tested and exercised on an annual basis.

Our plan calls for the notification of all employees of a facility that an event has occurred and where each employee is to report. We have a toll-free number for all Postal Service employees to use in the event of an emergency to receive information about facility closings and operating status.

We are updating the computer program which will identify critical postal facilities in the path of approaching storms, provide floodplain modeling, and real-time storm updates, as well as estimate anticipated impacts on postal assets.

The Inspection Service routinely works with other local and Federal law enforcement agencies. We also participate in training exercises. This ensures that postal employees, equipment, and procedures are ready to manage an emergency without interrupting operations.

The Inspection Service conducts and evaluates training on procedures for emergency management personnel and other essential staff. This promotes preparedness, improves response capabilities, assures that all systems are appropriate, and determines the effectiveness of our command, control, and communications processes.

Thank you for the opportunity to testify about some of the Postal Service's initiatives on safety and security. I would be pleased to answer any questions this subcommittee may have.

[The prepared statement of Mr. Cottrell follows:]

UNITED STATES
POSTAL SERVICE

STATEMENT OF GUY COTTRELL,
DEPUTY CHIEF POSTAL INSPECTOR,
BEFORE THE SUBCOMMITTEE ON FEDERAL WORKFORCE, POSTAL SERVICE
AND THE DISTRICT OF COLUMBIA
OF THE
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

MARCH 16, 2010

Good afternoon Chairman Lynch, Ranking Member Chaffetz and members of the Subcommittee. My name is Guy Cottrell, Deputy Chief Inspector for the United States Postal Inspection Service. I am pleased to be here with you today to discuss safety and security practices at the United States Postal Service.

In the Postal Service, many functions work together on the safety and security of our employees. While I am a postal inspector, please note that in discussing today's testimony, I am also providing information that reflects security strategies across many different functions, including Human Resources, Operations, Information Technology and Facilities.

Let me begin with the role of the United States Postal Inspection Service. Our mission is to protect the U.S. Postal Service and employees, secure the nation's mail system and ensure public trust in the mail.

As one of our country's oldest federal law enforcement agencies, founded by Benjamin Franklin, the United States Postal Inspection Service has a long, proud, and successful history of fighting criminals who attack our nation's postal system and misuse it to defraud, endanger, or otherwise threaten the American public. As the primary law enforcement arm of the United States Postal Service, the U.S. Postal Inspection Service is a highly specialized, professional organization performing investigative and security functions essential to a stable and sound postal system.

Congress empowered the Postal Service "to investigate postal offenses and civil matters relating to the Postal Service." Through its security and enforcement functions, the Postal Inspection Service provides assurance to postal employees of a safe work environment; postal customers of the "sanctity of the seal" in transmitting correspondence and messages; and American businesses for the safe exchange of funds and securities through the U.S. Mail.

Postal Inspectors are federal law enforcement officers who carry firearms, make arrests and serve federal search warrants and subpoenas. Inspectors work closely with U.S. Attorneys, other law enforcement agencies, and local prosecutors to investigate postal cases and prepare them for court. There are approximately 1,400 Postal Inspectors stationed throughout the United States and abroad who enforce more than 200 federal laws covering investigations of crimes that adversely affect or fraudulently use the U.S. Mail and postal system.

To assist in carrying out its responsibilities, the Postal Inspection Service maintains a Security Force staffed by approximately 650 uniformed Postal Police Officers who are assigned to critical postal facilities throughout the country. The officers provide perimeter security, escort high-value mail shipments, and perform other essential protective functions.

The Postal Inspection Service is responsible for the physical protection of all postal facilities, personnel, assets, and infrastructure. The Postal Inspection Service maintains liaison with other investigative and law enforcement agencies, including the Department of Homeland Security, the Federal Emergency Management Agency (FEMA), and other national emergency coordinators.

Today my testimony will focus on the Postal Service's building and employee security assessments, how threat communications are disseminated, the role that communications plays in securing employees' safety and the Postal Inspection Service's coordination with federal and local law enforcement.

One of the strengths of the Postal Service's safety programs is that they are reinforced locally. While headquarters provides national guidance, Area and District offices have personnel tasked with a variety of safety functions. The Postal Service's *Infrastructure Security Assessment Program* provides a good example of how functional experts work together with postal managers to take a comprehensive look at a building's security. The program was developed to help postmasters and installation heads achieve and maintain compliance with existing policies and procedures governing physical security, personnel security, internal security, and mail security. Tools used to conduct the review include comprehensive onsite observations, document reviews, and interviews of facility personnel. At the conclusion of each assessment, a plan is developed to address any issues identified in that review.

The same team approach is used when new postal facilities are being designed and when postal facilities undergo renovations. Postal Inspectors, working with staff from the Postal Service's Facilities office, assess risks to ensure that appropriate security and safety measures are incorporated into facility construction plans, assuring that facilities offer appropriate protection for postal employees, customers, and assets. In reviews of existing postal facilities, Postal Inspectors routinely identify issues with doors, windows, fencing and gates and offer recommendations to enhance security. In addition, each postal facility has a Security Control Officer who is responsible for the security of their facility and ensuring compliance with the Postal Service security policies and procedures.

One recent highlight is a new security computer system–the Enterprise Physical Access Control System (ePACS)–that links the Postal Service's computerized access control systems nationwide through its local area network. When actions are taken in one system, such as an employee termination or a suspension of access, they are reflected system-wide. This system is being deployed currently.

A key strategy that we use regarding enhancing security is to reinforce the key role that employees play in each other's safety. The best security force for any facility comes from the people who work in that facility. At every opportunity, the Postal Service has reinforced the personal responsibility that employees share in keeping our facilities secure. Historically, special emphasis has been placed on developing employee communications safety materials. Reinforcing communications with employees on safety matters is ingrained in our culture. Each week at facilities nationwide, managers are required to give safety stand-up talks. These talks are on the clock and provide employees with safety tips and information. During these talks, we use data that we have on trends or incidents that need to be emphasized with employees. We have developed safety posters, videos, and pamphlets. For example, regarding building security, we remind employees: "Remember, security begins with you. Help us protect your facility." Simple tips to employees such as looking at the condition of fences or lighting or deadbolt locks or public access to the workroom floor all contribute to employee safety. We will shortly begin an educational campaign aimed specifically at our letter carriers, to provide them with safety advice to increase their awareness while out of the office delivering mail.

Our Human Resources department maintains an Intranet site dedicated to safety. Employees can look up safety talks by topics or consult a fire drill evacuation checklist or review safety policies and procedures.

Another step in protecting employees and facilities is to ensure that a background check has been conducted regarding potential Postal Service employees. Postal Service Human Resource officials, working with the courts, law enforcement officials and background-check providers,

screen applicants for career-employee positions. The Inspection Service is responsible for conducting background investigations related to the issuance of security clearances for the Postal Service. Career and Contract Delivery Service personnel are fingerprinted, checked for a criminal history, screened for drug use, and verified for U.S. citizenship or legal work status. Emphasis on the security clearance process is important because a serious risk posed to most businesses comes from the "insider" who has access to restricted areas, knowledge of sensitive procedures, or access to sensitive information. Rigorous adherence to these procedures has helped maintain the Postal Service's position as one of the most trusted Federal agencies.

A major component of the Postal Service's workplace violence prevention program is the District Threat Assessment Team [TAT]. Threat Assessments Teams use cross-functional team approaches to assist in assessing threatening situations and to develop risk abatement plans to minimize the potential risk of future violence. Each District is responsible to establish and maintain a TAT to ensure that employees are aware of how to contact the TAT and share information. The TATs are violence awareness/prevention teams designed to ensure a safe working environment for all employees and a secure business climate for Postal Service customers. The Postal Service also requires supervisors to complete Workplace Violence Awareness training. The goal of the web based training is to provide supervisors with the keys to identifying and responding appropriately to reports of acts of violence and/or inappropriate behavior.

The Postal Service provides a vital service to America. The Inspection Service works with other law enforcement agencies when faced with a natural or manmade threat and/or disaster. The purpose of national preparedness planning is to ensure readiness and risk mitigation plans, and to return to normal operations as quickly as possible. This is accomplished internally by an all-hazards plan which designates teams at various organizational levels who are responsible to perform designated preparedness and response tasks specific to a particular threat or hazard.

The Postal Service has established and continues to refine an agency wide continuity program. A main objective of the program is to ensure safety and welfare of all Postal Service personnel throughout any incident. Today's threat environment and the potential for no-notice emergencies, including localized acts of nature, accidents, technological emergencies, and malicious attacks, have increased the need for this. The continuity program incorporates plans and procedures prior to, during and after an event relative to the employee's safety and welfare. The Postal Service Continuity Program components are tested and exercised on an annual basis.
The following are employee safety oriented components that support the Postal Service Continuity Program.

Prior to an event, procedures are implemented that allow for the notification of all employees of a facility that an event has occurred and where each employee is to report. The National Employee Emergency Hotline is one component of these procedures. This is a toll-free number for all Postal Service employees to use in the event of an emergency (facilities problems, weather emergencies, etc.) to receive information about facility closings and operating status. We are also updating another computer program – the Geospatial Information System Technologies – which identifies critical postal facilities in the path of approaching storms, provides flood-plain modeling and real-time storm updates, and helps estimate anticipated impacts on postal assets.

Immediately after an event, a determination is made as to whether a facility is safe for re-entry via the Facility Assessment Tool. This tool utilizes a cross functionally developed process to assess facilities for security, safety (physical and environmental) and health concerns. Additionally, the Postal Service has a national contract with a firm to allow the Postal Service to have expertise on call to mitigate or remediate any issues identified during the assessment.

As part of maintaining liaison with other federal and local law enforcement agencies, the Inspection Service works with other agencies on training exercises. This ensures that Postal

Service personnel, equipment, and procedures are ready to manage an emergency without interrupting operations. The Postal Inspection Service conducts, reviews, and evaluates training on proper procedures for emergency management personnel and other essential staff. Testing ensures that essential equipment and information systems, and the processes and procedures needed to use them, are viable and conform to proper specifications. The exercises promote preparedness, improve response capabilities for individuals and functions, assure that all systems are appropriate, and determine the effectiveness of command, control, and communications processes.

Additionally, the Postal Inspection Service helped implement the Federal Emergency Management Agency's (FEMA) National Exercise Schedule (NEXS), as the Postal Inspection Service is a stakeholder in the National Level Exercise and Principal Level Exercise. The Postal Inspection Service partnered with other federal agencies to collaborate, coordinate, critique, and provide essential feedback in support of its national response readiness operations.

Thank you for the opportunity to testify about some of the Postal Service's initiatives on safety and security. The Postal Service views employees as its most important asset and their safety is critical to us. We will continue to communicate the personal responsibility that employees need to take regarding their safety, while doing our utmost to provide secure work environments. I would be pleased to answer any questions the Subcommittee may have.

###

Mr. LYNCH. Thank you, Mr. Cottrell.

I now yield myself 5 minutes.

Director Goldstein, I had an opportunity to read your report from I think it was June 2009 where you did an assessment of the Federal Protective Service, and it was very, very helpful. I am not sure if it was a fair point in time to take a snapshot, however.

I know that up until 2007 the Federal Protective Service was in the process of scaling down, downsizing. And then Congress, in 2008, said stop downsizing, start hiring. We came in with a minimum staffing requirement of, I think, 1,400. So then FPS had to reverse what they were doing and start hiring, which they were not prepared to do, and that is when you took the snapshot, so there is some difficulty here transitioning from one function to the other, one policy to the other.

I am just wondering if you have had a more recent opportunity to do that analysis. I know you had folks, or perhaps you, yourself, went to various facilities and did this assessment. You talked to customers. You talked to a lot of people. I thought the report was fairly comprehensive in terms of the number of districts that you had reached out to, but is there a more recent assessment that you have made in terms of the readiness of the Federal Protective Service and its ability to meet Congress' more recent mandate?

Mr. GOLDSTEIN. Mr. Chairman, we have done a number of approaches over the years. In 2008, we issued a report which was sort of our more recent baseline report which, again, to reveal a lot of the issues that were coming about as a result of the downsizing that the agency was undergoing.

As you mentioned, since then a floor has been placed at 1,250 individuals, about 950 of whom must be law enforcement officers.

We have done additional work since that time. We issued a report on human capital planning at the Federal Protective Service. We did testimony, preliminary findings, which you are referring to from last summer in which we did a variety of things, including some penetration testing of Federal buildings, as well as looking at the contract guard program.

We will shortly issue a final report looking at those issues to a number of committees of Congress that requested that work. So we are continuing to do work on the agency, and there are some additional reports that Congress has requested that we also do, including taking a look at the transition into NPPD, as well as taking a look at RAMP and whether RAMP will be a successful program in helping the agency.

So we have continuing work on the way.

Mr. LYNCH. One of the problems that I have in assessing systemwide Federal security is that, for example, here on Capitol Hill, the legislative branch, we have the Capitol Police. We sort of have our own security system that we operate, as does the Federal court system. They sort of have the marshals inside the building, they have FPS outside. We have the Capitol Police. It is really sort of organic. DOD does their own thing, and so it is tough to take one measurement.

Is there a study or review that you are undertaking now that would help me with that, or are you just responding as requested from these different committees?

Mr. GOLDSTEIN. Most of our time up until now we have focused on the Federal Protective Service because of the GSA properties, but we have received recent requests from the House Homeland Security Committee to examine just what you are suggesting, which is more broadly taking a look at how security of Federal property across the entire spectrum is managed, who is responsible for it, how it interacts, how they coordinate, what kind of challenges they face. So we will be getting that work soon, sir.

Mr. LYNCH. All right. I guess what I am asking, Are there gaps in what we are requesting in order to get a good sense of what is going on and what the entire picture is here in the Federal Government?

Mr. GOLDSTEIN. We have recently received a number of requests from House Homeland Security which I think fills a lot of those gaps, but I will be happy to take a look at what we do have in that we are supposed to work on and talk with your staff about some of those gaps. Yes, sir.

Mr. LYNCH. That would be helpful. Thank you. Thank you, Mr. Goldstein.

The Chair now recognizes Mr. Chaffetz, our ranking member, for 5 minutes.

Mr. CHAFFETZ. Thank you, Mr. Chairman.

Mr. Goldstein, if we could start, you used the word confusion when you are talking about the interaction with local law enforcement responding to situations in Federal buildings. Can you expand on that just a little bit more, because there are multiple jurisdictions that often would respond to some sort of incident, but explain to us a little bit more what you meant by confusion that was out there.

Mr. GOLDSTEIN. Yes, sir. I would be happy to.

Several years ago in 2008, when we began discussions with the Federal Protective Service on their relationships with local police, at that time they explained to us that as they were decreasing the size of FPS they would be relying more on local law enforcement and entering into memorandums of understanding with local law enforcement around the country to assist them in times of emergency.

Over time, they realized that those MOUs probably would not be sustainable because many local law enforcement entities have enough of their own problems going on and would not wish to enter into such agreements, and that ultimately is what they found.

What they told us at the time is that they were continuing, however, to develop relationships with local law enforcement and that they had sort of more informal and ad hoc relationships to help them in times of emergency, and that I suspect is true. We often see local law enforcement responding to the scene when situations occur.

However, what has concerned us is we have done interviews in the course of our audit work in which we have spoken to precinct commanders, for instance, in a major metropolitan area literally within sight of level four Federal buildings, major level four buildings, who had no idea of when the last time they saw an FPS officer was, what kind of relationship existed with that building a

block or two blocks away, and what their responsibility would be in an occurrence.

Mr. CHAFFETZ. Let's do that. My guess is, my sense based on what the chairman was also asking, this is something we would like to explore further and learn a lot more about.

Mr. GOLDSTEIN. Yes, sir. We would be happy to explore that with the staff.

Mr. CHAFFETZ. That would be great.

Mr. GOLDSTEIN. Yes, sir.

Mr. CHAFFETZ. Can you help me, particularly Mr. Schenkel, understand, at least over the last 24 to 36 months, 2 to 3 years, what is the trend and the number of people that are working and helping to secure?

Mr. SCHENKEL. It has been very positive. When we got the relief as a result of the 2008 omnibus bill, we were able to hire an additional 150 FPS inspectors. In addition to that, we were able to revamp the training curriculum at the physical security training program, our in-house academy down at the Federal Law Enforcement Training Center.

Mr. CHAFFETZ. Again, I am sorry to cut you off. I have only got just 5 minutes and I want to touch on two other subjects. If you could provide us on the committee some additional details as to where that staffing is going for both the physical infrastructure and some of the other issues, that would be great.

And then if you could also, you mentioned the confiscation of 600,000-plus prohibited items?

Mr. SCHENKEL. Yes, sir.

Mr. CHAFFETZ. I would love to see what is on that list and if there is a detail as to how many knives or how many this or that.

Mr. Chairman, I am concerned about this, not only in these facilities but also at airports, as well. I think we need to look at what are we going to do about it. Is there enough of a deterrent, if you will, to try to get or bring these items in? I am sure a lot of these happen accidentally, but we are not talking about oversized shampoos here, is my guess. My guess is we are talking about something that is a little bit more nefarious in its nature.

I recognize the demand on the security personnel to have to be right all of the time, but I worry that these numbers are so huge. And I have heard similar things at the TSA, as well, so I would like to explore that and get additional information about that as we move forward, because that is just not acceptable to have so many prohibited items trying to be pushed and moved through the system. Obviously, there is room for error along the way.

My time is concluding here, so I yield back the balance of my time, Mr. Chairman.

Mr. LYNCH. Thank you. The Chair now recognizes Ms. Eleanor Holmes Norton for 5 minutes.

Ms. NORTON. Thank you, Mr. Chairman.

Mr. Schenkel, you are perhaps, I am sure—I should not even say perhaps—aware of Mr. Goldstein's testimony some months back where the GAO used testers who were able to smuggle bomb parts into, I think it was perhaps as many as 10 Federal facilities, take them into a men's room, and, if necessary, assemble them. Can you

tell this subcommittee today that has been corrected, since it is at least a year old, I think, that testimony was offered?

Mr. SCHENKEL. Yes, ma'am. We have taken dramatic steps as a result of that. We have taken a number of steps as a result of the penetration test that the GAO conducted, to include we initiated a gap analysis to identify where those problems came from. We revamped the x-ray magnetometer training. We have initiated the national weapons detection program, which is an additional 16 hours of magnetometer and x-ray training for all of our protective security officers.

We have also instituted the Covert Testing Working Group, which I mentioned in my initial testimony, where our individual criminal investigators, with a standardized uniform policy and a standardized uniform testing kit.

Ms. NORTON. Mr. Schenkel, we have a call into my office from someone who called himself a Federal Protective Services employee who said to us that the FPS plans to eliminate its HAZMAT program. Of course, these are the programs that monitor dangerous packages and provide training for such monitoring. Is the FPS planning to eliminate its HAZMAT program?

Mr. SCHENKEL. No, ma'am, it is not.

Ms. NORTON. Is it still the case that we have a proliferation of guards who remain stationary and cannot leave their posts, even to assist a Federal Protective Service officer?

Mr. SCHENKEL. It depends on the building and the responsibilities of that post.

Ms. NORTON. Who decides that, Mr. Schenkel?

Mr. SCHENKEL. It is a combination of the facilities security committee that writes the post orders and the relationships——

Ms. NORTON. The facility security committee within each building?

Mr. SCHENKEL. Yes, ma'am.

Ms. NORTON. That is my problem, Mr. Schenkel. You know, if you are very highly qualified employee at HHS, you don't know a hill of beans about security. The delegation of so much of security to internal committees almost guarantees that what Mr. Goldstein found will happen.

Mr. Schenkel, we know and there has been testimony that these guards not only can't leave their posts; they believe if they do leave their posts, even to engage in a chase on their own or assisting an FPS officer, they may face liability. Is that the case? Have they been told that if you leave your post, somebody is coming in with a gun, he runs, should the guard, not the FPS officer—you have a proliferation of guards, not FPS officers—should that guard run after that person who is trying to run away with a gun or with whatever he has in his hand?

Mr. SCHENKEL. That is an identified training gap that we take on the responsibility for. We have to ensure that those guards are aware that they are not on their own personal liability when those——

Ms. NORTON. Mr. Chairman, what is so scary about testimony after testimony is this has been the case ever since guards have been used. This is not the case, Mr. Goldstein. I mean, this could

have been corrected many years ago, but this policy of not leaving your post has been the policy all along, has it not, Mr. Goldstein?

Mr. GOLDSTEIN. That is my understanding, ma'am.

Ms. NORTON. How is it that, with the Congress having said you should have no fewer than 1,200 officers, Mr. Goldstein reports that the FPS officers are on something called reduced hours? Why would they be on reduced hours?

Mr. SCHENKEL. I am not aware of that, ma'am. If anything, they are on extended hours.

Ms. NORTON. Mr. Goldstein, you say in your testimony, you report reduced hours. That is where I got it from.

Mr. GOLDSTEIN. Yes, ma'am. What we are referring to is during the period of time certainly that the Federal Protective Service was reducing its personnel, its officers, the law enforcement security officers and the remaining patrol officers, FPS made a decision that in most places there would not be weekend hours, there would not be hours that——

Ms. NORTON. Mr. Schenkel, if there are Federal employees in a building during weekend hours, is there Federal Protective Service there during those hours?

Mr. SCHENKEL. It depends on the location, ma'am.

Ms. NORTON. And, again, who decides that, Mr. Schenkel?

Mr. SCHENKEL. It is a combination of the needs of the facilities, if they are isolated facilities, and/or of the region of they are in a regional facility. There is 24/7 covered here in——

Ms. NORTON. Mr. Schenkel, isn't it true that the internal committee is who basically is making these decisions, not your officers?

Mr. SCHENKEL. In some cases, but not in all cases.

Ms. NORTON. I think this is a very serious proposition, Mr. Chairman, that security is in the hands of civilians who happen to be sitting on these committees and who, given the power, is going to use it as they see fit. Is that not the case, Mr. Goldstein?

Mr. GOLDSTEIN. We have found a number of weaknesses with the building security committees, now called facilities security committees. They are made up of representatives from the tenant agencies. Usually the largest tenant agency in the individual building serves as the Chair.

I have attended a number of these meetings over the years, just to see how they operate, and, while I think they are well intentioned, and they certainly should have an advisory role, we have been concerned that you have a very balkanized, fragmented approach to the security of GSA's portfolio when every building gets to make significant decisions about how security is managed, as opposed to FPS being allowed to do a portfolio-wide approach that is based on risk management principles.

Ms. NORTON. You know, as competent and dedicated as, for that matter, a Member of Congress may be who is my colleague, I don't want a Member of Congress deciding security for entry into this building.

Mr. Chairman, may I just say finally in closing that the time has come, I think, for the committees who have been concerned about this to mandate that security be in the hands of trained security officials, and I would like very much to work with you, the ranking member, and to ask the members of the Homeland Security Com-

mittee and the Transportation and Infrastructure Committee, which also has some jurisdiction over FPS employees, to all get together. Maybe if we gang up on this problem we can get better security for Federal employees.

Mr. LYNCH. Thank you. I think that is a great suggestion about a joint effort, maybe joint hearings going forward. That is a great idea.

The Chair now recognizes the distinguished gentleman from Virginia, Mr. Connolly, for 5 minutes.

Mr. CONNOLLY. Thank you, Mr. Chairman.

Mr. Schenkel, you talked about the Federal Protective Service conducting sort of fixed-post and roving patrols of Federal facilities. Are there other things preventively that the Federal Government can or should do, the FPS in particular, to try to anticipate and/or prevent possible terrorist attacks?

Mr. SCHENKEL. Sir, FPS takes an integrated approach that we actually start using international and national intelligence resources. We have access to that through our regional intelligence agents. They provide a threat picture, a threat analysis, if you will, of each facility. That is coupled with local law enforcement and we get the predictions and threat analysis also from them and take that approach even further.

We employ certain countermeasures that could be cameras, intrusion detection systems. Obviously, our most visible countermeasure is the armed contract protective security officer, and certainly our most professional and most proficient is our armed Federal Protective Service law enforcement security officer.

Mr. CONNOLLY. You make reference to the MOUs with local law enforcement, but Mr. Goldstein, if I understood your testimony, you raised some concerns about the sustainability of those MOUs, given the already heavy burdens borne by local law enforcement. Are those MOUs, with all the good intentions of the world, something we can count on to help protect our Federal employees?

Mr. GOLDSTEIN. It is my understanding that, because of the difficultly arising from gaining commitments out of local law enforcement, that there are few, if any, MOUs that are actually in place, and that I think Mr. Schenkel can tell you that generally what they strive to do is create relationships with local law enforcement in some of the major metropolitan cities where risks are higher. But, again, we found some concerns, even in places where they had done that, that, while they have tried to do that, the communication and interaction necessary to ensure collaboration wasn't always in place.

Mr. CONNOLLY. Mr. Schenkel, did you want to comment on that?

Mr. SCHENKEL. Mr. Goldstein is correct. It is difficult to get an MOU with a metropolitan law enforcement agency. Having come from one myself, I understand that difficultly because of the liability issues. However, we have not had a single instance in FPS, at least during my tenure, that we have had any difficultly in coordinating or occupying a facility when there is a threat. We have normally developed a command and control situation where FPS will take command and control of the situation of a Federal facility when local law enforcement responds.

Mr. CONNOLLY. Are the rules of engagement fairly clear between the FPS and the local law enforcement agencies? I can think of some events right here in the national capital region where the lines of authority become an issue in terms of whose turf are you on and whose the primary responsibility for X, Y, and Z in terms of security. I won't name what, but it can sometimes be an issue. Is that an issue sometimes for the FPS?

Mr. SCHENKEL. That will continue to be an issue wherever any law enforcement or two units operate together; however, in our case, because 80 percent of our facilities are leased facilities, there is an obligation by local law enforcement to respond just as a local fire department is required to respond, and we coordinate those activities either through Federal Protective Service officers on the ground or through our mega centers, our communication and dispatch centers that all 9,000 of our buildings are tied in to.

Mr. CONNOLLY. Mr. Miller, in your testimony you indicated that there really was not much we could have done to prevent the attack in Austin, if I understood your testimony.

Mr. MILLER. I believe that is right, sir.

Mr. CONNOLLY. I assume you meant by that physically once someone decided to take his airplane and flying into the building, there just wasn't much we could do.

Mr. MILLER. Yes, sir.

Mr. CONNOLLY. You were talking about the physical ability to restrain that individual once he got in his airplane?

Mr. MILLER. That is what I was speaking of, sir.

Mr. CONNOLLY. But are there other things—you heard me in my opening statement. One of the concerns I have is that there are some people in the media and even in political life who have, presumably unwittingly, nonetheless empowered some people who might be on the edge emotionally anyhow, to think it is OK, if it is a Federal agency you don't like, to fly an airplane into a building. Are there things outside of the physical challenge once someone decides to do something we can or should be doing or anticipating to try to ameliorate or mitigate any possibility of such attacks?

Mr. MILLER. I would think, Congressman, that there are others at this table and otherwise that would be better. Obviously, there is tracking of intelligence and Internet catch and all of that. That sort of isn't within the IRS' purview, and I think we would look to other experts for that sort of explanation and help.

Mr. CONNOLLY. I know my time is up, Mr. Chairman. If I might ask if there is anyone else at the table who wanted to respond to that.

[No response.]

Mr. LYNCH. No takers.

Mr. CONNOLLY. Thank you.

Mr. LYNCH. All right. Thank you, Mr. Connolly.

First of all, Mr. Miller, my condolences for the loss of life.

Mr. MILLER. Thank you, sir.

Mr. LYNCH. I know Vernon Hunter was a Vietnam veteran, two tours of duty, very close to retirement, so there is a human dimension here that sometimes gets lost in all of this.

Let me ask you, Ms. Armstrong and Mr. Miller, after the incident in Austin, as Mr. Connolly pointed out and you confirmed, there

was a certain unforseeability, this was so bizarre, I understand the evacuation and the post-attack procedures seemingly went very well. Were there any changes that you adopted, Mr. Miller, in terms of the way you are doing business at the IRS within some of your facilities? Was there a reassessment that you did following that event?

And, Ms. Armstrong, I understand that the Interagency Security part of this, its function is to make sure best practices are adopted across agencies.

Mr. Miller, is there anything that you did or the IRS did in response?

And Ms. Armstrong, was any of that translated across agency lines?

Mr. MILLER. Sir, I can speak to the IRS, Mr. Chairman. What we did almost immediately was increase the amount of security at all of our facilities until we were certain, during the weekend and a little later than that, because this happened late in the week on a Thursday, until we were sure that this was not a series of, the first of a series.

We then have continued additional guard service and additional security awareness and security at all the facilities, especially in Austin, but across the country, as well.

We are in the process of doing what you are suggesting, which is reassessing exactly where we are today, what is the general threat level with respect to IRS facilities, and do we have in place the processes and security we need to ensure the safety of our folks.

Ms. ARMSTRONG. Yes, sir. In terms of the actual incident in Austin, itself, as the Office of Infrastructure Protection we monitor all such incidents as they relate to Government facilities or a whole host of different types of issues that impact critical infrastructure, so we monitored the incident, reported again to the point of is this a series of attacks, up to the national operations center and our Secretary.

In terms of the Interagency Security Committee, this incident and other recent incidents are certainly part of the ongoing dialog that the committee is having about how it gets to the final stages of a couple of years of work to put together a ground-breaking compendium of standards for physical security at Federal buildings.

The Congresswoman mentioned the facilities security committee. That is actually the third piece of our work, the first two pieces being the physical security criteria for Federal buildings and then a design basis threat piece so that 31 different types of threat can be considered as a facility considers countermeasures.

What we are hoping to do with the facilities security committee is take 15 years worth of lessons learned on what is not working in terms of Federal Security Committee composition, training, and guidance, and have the Federal Protective Service and GSA co-chair the working group that looks at the whole issue of Federal Security Committees, how they work, what guidance they need, what training they need, and who needs to be on them to make effective security decisions at Federal buildings.

Mr. LYNCH. OK. Let me just followup on that. I understand that the Interagency Security Committee is sort of a facilitator across

agency lines, and I know it is responsible for coordinating security in all the non-DOD executive branch agencies, which is fairly expansive. You are talking millions of employees.

Ms. ARMSTRONG. Yes, sir.

Mr. LYNCH. And I also understand that you have one employee, one staff person, the ISC, that handles all of that. Now, at one point there was only one employee to do all of that. Have you increased staffing to get this thing done in light of the threat that is out there?

Ms. ARMSTRONG. Yes, sir. As you know, the Interagency Security Committee chair came to the Office of Infrastructure Protection in fiscal year 2008, and since then we have been resourcing it out of hide, if you will. We do have one Federal employee and a team of contractors who do the staff work of the ISC. But the ISC is a 45-member interagency body, and other Federal agencies provide subject matter expertise, personnel, brain power, and do the actual work of the committee. So we coordinate, but the whole interagency contributes in terms of resources.

Mr. LYNCH. OK. I am just interested in seeing that properly resources. If there is a weak link in this chain, it is probably that, so it is tough enough with so many players here. You definitely need somebody coordinating all that. For now we will leave it to the agencies to properly resource that, but we will keep an eye on it.

I now recognize the gentleman from Utah, Mr. Chaffetz, for 5 minutes.

Mr. CHAFFETZ. Thank you.

First, Mr. Chairman, if I could, with all due respect to Mr. Connolly, I could use some help with the clarification in both the opening statement and in the questioning as to the source of where potentially some of this terrorism and acts of violence are coming from.

Mr. LYNCH. You are not allowed to ask other Members questions. We brought in five witnesses here, and you can ask them. I guess that is why we have the witnesses here. So if you want to sort of probe that with the witnesses, because I think Mr. Connolly was asking folks or citing that. So if you want to ask the witnesses about that, that would certainly be relevant.

Mr. CHAFFETZ. I appreciate it.

Mr. LYNCH. And I understand the sensitivity here, and I have tried not to impugn or imply any particular source. I am actually working from the side of protecting the Federal employees within those facilities, and not working from the point of the folks that might be motivated to do something like this.

Mr. CHAFFETZ. Coming into this hearing, that wasn't my intention, either. It is just the idea of the suggestion that there was any Member of this body that would suggest or condone or even encourage somebody, I just wanted to make sure that he had that opportunity to help clarify. But we will move on here.

There was a suggestion in David Wright, who is the President of the Federal Protective Service Union, in his comments that the Federal Protective Service having been "slashed to the point of ineffectiveness." I wanted to give the FPS an opportunity to kind of

respond to that assertion that it had been slashed to the point of ineffectiveness. Would you care to comment?

Mr. SCHENKEL. I can't agree entirely with President Wright in regards to that. What I can say is that we had to refocus our protection mission, based on the available resources that we had. We got involved in some things through mission creep, as I would call it, that got us distracted from the facilities that we were charged to protect. Consequently, we had to revamp our strategic plan and focus on the protection of the facilities. It is a challenge. It is a constant maneuvering of resources that we have that are available. As the threat changes, we have to keep maneuvering those limited resources where possible.

Mr. CHAFFETZ. Thanks. I yield back the balance of my time.

Mr. LYNCH. Thank you.

The Chair recognizes Ms. Eleanor Holmes Norton for 5 minutes.

Ms. NORTON. Thank you, Mr. Chairman.

Ms. Armstrong, as you can see, the Interagency Security Committee bugs me. And I do want to make it clear that when Mr. Schenkel talks about the gap—and I think he is candid in reporting a gap—the gap should be labeled for what it is. It is a gap between burdensome and unnecessary security on the one hand and lax security on the other.

The example that I offered before at the Department of Transportation—and let me tell you how this plays out. This is a fairly new facility. It is located along N Street Southeast. There are 20 million tourists and visitors who come to the District of Columbia. If you go along that street, we are just filling it out with the kinds of shops that you might expect and will be there over the years.

Imagine yourself as a visitor to our city and you say, well, there is a Federal building, Johnny. We can go to the bathroom there. And I am telling you that because an interagency committee has some kind of hubris of self-importance, that taxpayer who paid for that building cannot enter that building because somebody has decided—and we understand that the center of authority is in this committee—that a taxpayer can't get into that building unless the taxpayer knows a staff person who can come down and give the OK for the person to enter the building. Do you consider that appropriate, that kind of entry requirement for ordinary, law-abiding citizens to be appropriate?

Ms. ARMSTRONG. Well, I think the key there is what is the agency, what is the——

Ms. NORTON. I am giving you an example and I would like you to answer my example, not depending on the agency. I have given you a low security agency and I am asking you whether you consider it appropriate that a taxpayer with a child, or without a child, cannot get into that building to use the facility or, for that matter, to go to the cafeteria. Do you consider that appropriate?

Ms. ARMSTRONG. Well, I think it is appropriate to have security practices and procedures in place that would prevent the unauthorized entry of an unauthorized person into a Federal facility.

Ms. NORTON. And you don't consider the taxpayer I am talking about an unauthorized person, would you?

Ms. ARMSTRONG. Well, I don't know the actual person that you are talking about.

Ms. NORTON. Mr. Chairman, this is what I mean. I have given you a hypothetical. You refuse to give me an answer to my hypothetical. Ordinary citizen with a child, should that ordinary citizen be able to enter the Department of Transportation building in order for the child to use the facilities? Yes or no?

Ms. ARMSTRONG. I would have to say no, ma'am.

Ms. NORTON. For what reason, Ms. Armstrong?

Ms. ARMSTRONG. For purposes of protecting the employees at that building.

Ms. NORTON. In which way would this taxpayer be considered a risk to the employees in that building?

Ms. ARMSTRONG. Well, if he were the ex-husband of a woman that he had abused and is using a ruse to try to get past security to get to her, then security——

Ms. NORTON. You see, Mr. Chairman, what I mean. Meanwhile, if this is the way you do security, Ms. Armstrong, I don't want you in charge of my security. I want somebody who, as Mr. Goldstein said, has taken a risk assessment and has decided is there a risk that a parent entering the building poses, a security threat, or is there a more serious risk.

Let me ask you, Mr. Schenkel, particularly in light of that answer, according to Mr. Goldstein's testimony—and I am reading—in 2008, FPS transitioned to an inspector—understand FPS, oldest Federal police force in the United States—the FPS transitioned to an inspector-based work force—this is page 6—eliminating the police position, and is relying primarily on FPS inspectors for both law enforcement and physical security activities, which has hampered its ability to protect Federal officials. In essence, this testimony from Mr. Goldstein says that the Federal Protective Service is no longer a police force, it is an inspector-based work force.

Since 2008, have you right-sided the agency so that the Federal Protective Service is today a police force and not an inspector-based force?

Mr. SCHENKEL. The inspectors are police officers.

Ms. NORTON. I understand exactly that. These are people who were patrolling before, who were looking for people like the bomb makers that Mr. Goldstein said, who were looking to prevent criminal activity. They were switched to a new position called an inspector position. My question to you is: have you switched any of these inspectors back to patrolling buildings and to being police officers, as they always were before this transition?

Mr. SCHENKEL. In some regions the inspectors do take the active patrol.

Ms. NORTON. What is your intent? Is your intent that the Federal Protective Service do engage in these patrols and not be an inspector-oriented-based work force as it had become?

Mr. SCHENKEL. It is a matter of resources, ma'am. We had to get the facilities——

Ms. NORTON. If it is a matter of resources, why aren't the resources put on the police part of the protective service as opposed to the inspector part of the protective service?

Mr. SCHENKEL. Because 80 percent of our facilities are protected by local and State law enforcement agencies, and with the resources that we have available——

Ms. NORTON. Mr. Chairman, my time is up. That is just not true. Local police forces do not protect Federal facilities. I just want to say for the record, Mr. Schenkel, that is untrue. The D.C. Police Department will not, in fact, protect Federal—and there has already been testimony here they all think they have liability. Let me tell you what else, Mr. Schenkel: they all have a lot to do protecting their own cities. So for you to sit here and say we depend upon the D.C. police force and the Fairfax police force to protect Federal facilities is quite an outrage.

Thank you, Mr. Chairman.

Mr. LYNCH. I thank you.

The Chair now recognizes the gentleman from Virginia, Mr. Connolly.

Mr. CONNOLLY. Thank you. Thank you, Mr. Chairman. I know we want to get on to some other witnesses, as well. I just have one question.

Ms. Armstrong, what does the Interagency Security Committee do to preempt or prevent violence against Federal facilities? Is it all on the physical structural side of hardening facilities, or do we get into other kinds of strategies in the preemption and prevention?

Ms. ARMSTRONG. We do get into the prevention area and we, in fact, have a working group on workplace violence working on issuing a compendium of best practices.

Mr. CONNOLLY. And presumably you are also plugged into some kind of stream of intelligence in terms of possible known threats or purported threats?

Ms. ARMSTRONG. Yes, sir. We use the Homeland Infrastructure Threat and Risk Analysis Center [HITRAC], which is part of the Office of Infrastructure Protection and the Office of Intelligence and Analysis at DHS, to help with the design basis threat that we will be issuing soon.

Mr. CONNOLLY. Thank you.

Ms. ARMSTRONG. Yes, sir.

Mr. CONNOLLY. Thank you, Mr. Chairman.

Mr. LYNCH. Thank you.

I yield myself 5 minutes.

Mr. Cottrell, this sort of gets to Ms. Eleanor Holmes Norton's issue. You have a situation where, with the Postal Service, the public is actually invited into the building, not for the bulk mail facilities but the regular post offices, even the large GMF facility at South Station. They have a big section there where they invite the public in, obviously. How do you handle that balance between maintaining security as you need to, taking in packages from the public, as well, and yet maintaining the security for your personnel?

Mr. COTTRELL. It is a challenge, Mr. Chairman, but to balance being a retail facility as well as a Government facility and protect employees, we rely on training—training our supervisors and employees how to recognize and react to potentially violent encounters.

We don't experience many breaches of security into the back rooms of facilities, but, as you stated, we do have several, well, we have thousands of retail facilities where sometimes unhappy cus-

tomers can come in and attack or assault our employees. So it is really an awareness training of what to watch for and making sure our employees know who to contact and the steps to take if such an incident does occur to try to de-escalate or report an incident.

Mr. LYNCH. I also know that there is, at some level, some coordination between the U.S. Postal Service and DHS. I was involved with the installation of some of the new technology that was put in place after the anthrax attacks here at the Brentwood facility and elsewhere, I think in New York, but how has that coordination worked out? Was that a one-time event or is that something that is ongoing?

Mr. COTTRELL. It is ongoing. We participate in the ISC, the Interagency Security Committee, and, truthfully, the anthrax attacks, really. The Postal Service learned a lot of valuable lessons about liaisoning with other Federal, State, and local agencies so that folks know what to do. That is part of our annual training is to work and liaison with these other agencies.

Mr. LYNCH. OK. You know, we have one more panel to come up here. I think all of you know we didn't have much time to put this hearing together. I appreciate the thoroughness of your written testimony.

I will leave the record open so if some Members who were in another hearing, I know Budget Committee is meeting right now, as well, and some of our Members are on that committee. But I want to thank you for your willingness to come before Congress and to offer your suggestions to possible solutions. We will be working on this going forward, probably in coordination with the Committee on Homeland Security, Mr. Thompson, so you may receive some requests in writing for testimony, further testimony, and to answer further questions.

Thank you for your testimony here today, and I wish you a good day.

All right. Panel two. First of all, let me welcome you to this hearing. I appreciate your willingness to come before this subcommittee with your testimony. What I will do is I will read a brief introduction of our witnesses, and then we will open it up for questions after you are sworn.

Colleen Kelley is the president of the National Treasury Employees Union, the Nation's largest independent Federal sector Union, representing employees in 31 different Government agencies. Ms. Kelley, a former IRS revenue agent, was first elected to the Union's top post in August 1999.

Jon Adler has been the national president of the Federal Law Enforcement Officers Association since November 2008. He began his career in law enforcement in 1991 and has served as Federal criminal investigator since 1994. His experience includes working a wide variety of investigations and enforcing most of the Federal criminal statutes.

Mr. David Wright is the president of the American Federation of Government Employees, Local 918, the National Federal Protective Service Union. Mr. Wright is also a veteran Federal Protective Service Officer and Inspector for over 20 years.

It is the custom within this committee to ask all those who are to offer testimony to be sworn, so may I please ask you to rise and raise your right hands.

[Witnesses sworn.]

Mr. LYNCH. Let the record reflect that each of the witnesses has answered in the affirmative.

Ms. Kelley, you are now recognized for 5 minutes for an opening statement.

STATEMENTS OF COLLEEN KELLEY, NATIONAL PRESIDENT, NATIONAL TREASURY EMPLOYEES UNION; JON ADLER, NATIONAL PRESIDENT, FEDERAL LAW ENFORCEMENT OFFICERS ASSOCIATION; AND DAVID WRIGHT, PRESIDENT, LOCAL 918, AMERICAN FEDERATION OF GOVERNMENT EMPLOYEES

STATEMENT OF COLLEEN KELLEY

Ms. KELLEY. Thank you, Mr. Chairman, Ranking Member Chaffetz, and members of the committee. I am very pleased to be here on behalf of NTEU to discuss Federal employee workplace safety and security issues.

As you know, on Thursday, February 18th, in what authorities believe was an intentional suicide attack, a pilot with a perceived grudge against the Government, in general, and the IRS, in particular, crashed his small plane into a building housing almost 200 IRS employees and NTEU members in Austin, TX.

As has been noted, the attack took the life of Vernon Hunter, a 27-year IRS employee, a beloved husband, father, grandfather, and U.S. veteran. Vernon's wife, Valerie, works for the IRS, as well, and was also in the Echelon building when the plane hit. They both have been long-time NTEU members, and I share in the sorrow that this tragic loss has caused for their family and for so many others.

I know many of you saw pictures on TV of the Austin IRS building engulfed in flames and probably wondered, as I did, how so many people were able to escape, but I am guessing that many thought about it for a brief time and understandably moved on to other things. I think hearing what went on immediately after the attack may help to increase the urgency of preventing this from happening again and ensuring that employees know what to do if it does.

Treasury Secretary Geithner, IRS Commissioner Shulman, and I visited with the affected employees shortly after the attack and we heard incredible stories of terror and heroism that I would like to share with you.

Upon impact, the burning fuel from the plane quickly filled the air with black smoke, making it impossible for many in the building to see anything, yet employees near exits delayed their own escape so others could follow their voices and find their way out. Employees who were outside the building went back in to help evacuate disabled employees who worked in the mail room. An IRS employee with a disability told her co-worker to leave her on the fourth floor because she could not walk down the stairs. He insisted she climb on his back, saying he had carried soldiers that

way when he was in the service. He carried her on his back down the four flights to safety.

Andrew Jackson and Morgan Johnson and four others were trapped on the second floor of the building, unable to get to the exit because of the smoke, flames, heat, and debris. They crawled on their hands and knees, breathing through clothing they had dampened with water, looking for a way out. Morgan shouted through a broken window and got the attention of Robin DeHaven, who was an employee of a glass company who was miraculously passing by with a 20-foot ladder on his truck.

Robin, who was later dubbed Robin Hood by those that he rescued, stopped and he tried to reach the trapped employees, but the ladder could not reach to the window that had already been broken. Andrew remembered a 4-foot metal crowbar that was used for property seizures that was kept in the office. After a few attempts and several gashes to his hand and his wrist, Andrew and the others succeeded in breaking a window through which they could get out and reach the ladder, clearing the glass and helping each other down Robin DeHaven's ladder to safety.

Mr. Chairman, I have included in my written testimony several detailed suggestions on improving safety and security for the Federal work force, including increased staffing and training for the Federal Protective Service. NTEU is also requesting that the IRS undertake and include employees in a comprehensive review of safety and security measures at all of its facilities around the country, many of which have no guard or armed presence at all. And we want to make sure that IRS employees have access to any information on taxpayers who may pose a threat to their safety as they perform their duties.

But I would also like to urge this committee to take the lead not just on the issue of physical safety, but on the issue of holding public officials to a responsible level of discourse when it comes to the Federal Government and those who work for it. I have to say that I was shocked to hear comments from elected officials that expressed empathy for the man responsible for the horrific attack in Austin that took the life of a wonderful patriotic American who was carrying out the laws that this Congress writes.

I am not asking for limitations on free speech rights, but I am asking for members of this committee and this Congress to forcefully denounce this kind of irresponsible rhetoric before it contributes to more misguided violence against Federal workers who are just doing their jobs.

Mr. Chairman, I know that you and other members of this committee have spoken out forcefully on this issue, and I very much appreciate that. I also appreciate the strong statement of support from President Obama. And NTEU appreciates the fact that the House passed a bipartisan resolution authored by Congressman Doggett of Texas supported by members of this subcommittee with you, Mr. Chairman, as an original coauthor, condemning the attack in Austin. I thank you for that and I thank you for holding this important hearing. I hope it will encourage others to join in these efforts, and I would be happy to answer any questions.

[The prepared statement of Ms. Kelley follows:]

Statement of Colleen M. Kelley

National President

National Treasury Employees Union

On

"Federal Employee Workplace Safety and Security"

Submitted to

House Committee on Oversight and Government Reform
Subcommittee on Federal Workforce, Postal Service and the District of Columbia

March 16, 2010

1750 H Street, N.W. • Washington, D.C. 20006 • (202) 572-5500

Chairman Lynch, Ranking Member Chaffetz, and distinguished members of the Subcommittee, I would like to thank you for allowing me to provide comments on federal employee workplace safety and security. As President of the National Treasury Employees Union (NTEU), I have the honor of representing over 150,000 federal workers in 31 federal agencies and departments.

Mr. Chairman, recent events have once again raised concerns about the vulnerability of federal buildings and the safety and security of federal employees who work in them around the country. As you know, on Thursday, February 18, in what authorities believe was an intentional suicide attack, a pilot crashed his small plane into a building housing almost 200 IRS employees in Austin, TX. The attack, in which one IRS employee lost his life and several others were seriously injured, serves as a grim reminder of the great risk that federal employees face each and every day in service to this country.

Data from the Treasury Inspector General for Tax Administration (TIGTA), which is charged with investigating threats and assaults against IRS personnel, show that IRS workers are among the most targeted group of federal employees due to the nature of their work, which often requires close interaction with the public. According to TIGTA, more than 1,200 threat and assault cases were referred to TIGTA for investigation between 2001 and 2008. The cases resulted in more than 167 indictments and at least 195 convictions.

In addition, in recent years, several high profile cases in which disgruntled taxpayers have threatened to kill IRS employees or blow up IRS offices, further underscore the real and constant danger that IRS employees must face every day as they carry out their duties.

This incident also further heightened ongoing concerns by many federal employees that current safety and security standards at many federal facilities are insufficient.

Federal Building Security

Mr. Chairman, as you know, the responsibility for ensuring the physical safety of federal employees who work in roughly 9,000 federally owned and leased facilities is given to the Federal Protective Service (FPS), within the Department of Homeland Security. Part of that responsibility also includes ensuring the security of U.S. citizens who visit many of the federal workplaces. On any given day, there can be well over one million people who are tenants of, and visitors to, federal worksites nationwide.

Unfortunately, recent reports in the media, congressional testimony by the Government Accountability Office (GAO), and numerous conversations with federal employees represented by NTEU raise concerns that government employees and members of the public are not receiving the proper level of protection from the FPS. In particular, NTEU believes that inadequate funding, staffing and training at the FPS have hampered its ability to carry out its core missions to protect facilities, to complete building security assessments in a timely and professional manner, and to monitor and oversee contract guards.

According to the GAO, the FPS workforce has decreased about 15 percent from almost 1,400 employees in FY 2004 to about 1,200 employees at the end of fiscal year 2009. Given that there are approximately 9,000 federally-owned and leased buildings to protect, the FPS also contracts

with nearly 15,000 guards who handle the bulk of security at these facilities. In recent testimony before Congress, GAO also expressed concern that FPS was unable to properly manage these contracts.

But despite these warnings, in September of last year GAO released the preliminary results of a review of the operational and management challenges facing the FPS which found that federal employees, buildings and visitors may be at risk due to unqualified contract guards who were also lacking proper certifications. Additionally, GAO reported that FPS was still not providing sufficient oversight of the contracts of FPS personnel. Most troubling, GAO identified substantial security vulnerabilities related to FPS's guard program, including instances where explosive materials were able to successfully pass undetected through FPS monitored security checkpoints.

FPS officials have admitted that with limited law enforcement personnel, the agency is reduced to serving a reactive role, rather than a proactive force patrolling federal buildings and preventing criminal acts. The majority of contract guards are stationed at fixed posts, which they are not permitted to leave, and they do not have arrest authority. FPS has also reduced the hours of operation for providing law enforcement services at many federal buildings, resulting in a lack of coverage when employees are coming and going, and during weekend hours.

While we understand that FPS has met a congressionally-mandated staffing level of 1,200 employees, 900 of whom are required to be full-time law enforcement professionals, NTEU remains concerned that this number falls far short of the number of federal law enforcement officers necessary to secure roughly 9,000 federal buildings and maintain proper oversight of 15,000 contractors.

That is why we were disappointed to see that the Administration's budget request for FY 20011 includes no additional funding for the FPS above the FY 2010 level and proposes eliminating the minimum staffing standards previously established by Congress.

The importance of providing adequate security at federal buildings is of great concern to NTEU and our members who have repeatedly voiced their concerns about the safety of their workplaces, their own personal safety and that of the visiting public. NTEU strongly believes that only by providing FPS with increased staffing can we ensure that they are able to carry out their mission of securing federal buildings and ensuring the safety of the thousands of federal employees they house daily.

NTEU believes the transfer of FPS from U.S. Immigration and Customs Enforcement (ICE) to the National Protection and Programs Directorate (NPPD) will help FPS better focus on its primary mission of securing GSA owned and leased federal buildings by performing building security assessments and deploying appropriate countermeasures.

Security at the IRS

Mr. Chairman, as the Federal inventory of buildings has steadily increased over the last 30 years, the uniformity and implementation of security standards have varied greatly. Prior to 1995, minimum physical security standards did not exist for nonmilitary federally owned or leased facilities. But

even with established minimum safety standards, security at federal facilities can vary greatly from agency to agency and even from building to building.

This is particularly true for agencies like the IRS, which must offer public access to provide customer service. The IRS is widely dispersed with approximately 755 facilities throughout the nation. These facilities can range from one-person offices to large tax return processing campuses with thousands of employees. There are also different tenant sharing arrangements at these facilities, from being housed as an IRS-only office to sharing building space with other Federal agencies and other private companies. In buildings where the IRS is not the lead agency or tenant (i.e., the largest organization in the building) the IRS must propose changes through a building security committee.

NTEU members have consistently voiced concern over the inconsistency of safety and security measures at IRS facilities across the county, in particular, at facilities like Taxpayer Assistance Centers (TACs) which must offer public access in order to provide customer service. In many instances, there is an absence of any type of security presence at these TACs, which has heightened fears among employees that they are particularly vulnerable to threats and attacks.

Unfortunately, IRS has been slow to recognize the importance and necessity of providing a security presence at all IRS facilities. In fact, just recently, in the face of strong opposition by NTEU and our members, the IRS was forced to abandon an initiative to "standardize" its use of contract guards and dogs at various locations across the U.S., which would have resulted in the elimination or reduction of guard service at 42 posts. While NTEU was successful in fighting this planned reduction of guard services, many IRS facilities remain woefully unprotected. According to IRS, of the roughly 755 IRS facilities located nationwide, just 275, or 36%, have some type of security detail. Thus, 480 IRS facilities, roughly 64%, are without any security presence whatsoever. This is clearly unacceptable.

Mr. Chairman, the absence of adequate security at IRS locations is just one of many security related concerns reported by NTEU members in recent years, which also include: IRS taxpayer walk-in centers without metal detectors, or operational, monitored security cameras; insufficient perimeter lighting; inoperable security equipment; parking areas without security camera coverage; security service spread thin by guards required to leave their posts and patrol loading docks during deliveries; security devices ordered but uninstalled due to inadequate funding; malfunctioning security cameras, security gates and magnetometers; IRS walk-in centers with only cipher locks on the front doors; open loading docks without a security presence; excessive waits for security personnel arrival after making an emergency call; security cameras discovered to not have film after a robbery; and inoperable fire alarms.

As you can see, IRS workers' concerns about the heightened risk of threats and attacks at IRS facilities, in particular, at those which must offer public access in order to provide customer service, are not unfounded.

Mr. Chairman, I would like to state my appreciation to IRS Commissioner Shulman and Treasury Secretary Geithner for their efforts in the aftermath of the Austin IRS attack and I am hopeful that we can build on those efforts to improve worker safety at the IRS.

NTEU Recommendations

In an effort to help IRS minimize the threat of violence against IRS employees as they administer the Internal Revenue Code, NTEU proposes the following recommendations:
(1) IRS undertake a comprehensive review of safety and security measures at all IRS facilities; (2) ensure IRS employees have access to any and all information on those individuals that could pose a threat; (3) grant law enforcement officer (LEO) status to IRS Revenue Officers.

Comprehensive Review of Safety and Security Measures at all IRS Facilities

In light of recent events and ongoing concerns by IRS employees about their safety and the security of IRS locations, NTEU believes that IRS should immediately undertake a comprehensive review of safety and security measures at all IRS facilities around the country. In particular, IRS should review the current established physical security standards and requirements for the protection of Service facilities and personnel. The review should consider whether or not each facility has, among other things; the proper risk assessment security level designation; sufficient entry control systems, including guard or other armed presence and magnetometers; sufficient perimeter security, exterior lighting, proper designation of restricted areas, and operable security equipment.

We also believe that to the greatest extent possible, IRS should solicit the participation by IRS employees themselves in the review as they may be able to offer a unique perspective on the problems and challenges associated with securing IRS facilities, its employees, as well as the taxpayers who frequent them.

Input from employees on the front lines can be particularly helpful as the security needs at IRS facilities can vary greatly, depending on their mission, size, etc.

As the Internal Revenue Manual notes, in order to ensure that a Post of Duty (POD) is properly protected, careful planning is necessary to ensure that appropriate protective measures are in-place and tailored to the facility's specific mission, threat, and functional requirements. PODs may vary greatly in size and function, so each requires close examination for tailored security countermeasures. The function of the office, the type of records maintained, the equipment in the POD, the size, population, if visitors frequent the facility, etc., are all determining factors to consider when planning security.

Mr. Chairman, NTEU believes that it is important for IRS employees to feel safe and secure in the workplace as they carry out their duties and stands ready to work with the IRS to ensure the proper safeguards are in place to ensure the safety of IRS employees.

Ensure IRS Employees Have Access to Information

As you may know, the IRS Restructuring and Reform Act of 1998 (RRA 98) required the IRS to stop designating taxpayers as Illegal Tax Protesters (ITP) or any similar designation. This ITP designation was used previously by the IRS to identify individuals and businesses using methods that were not legally valid to protest the tax laws. The designation was also intended to alert employees to be cautious so they would not be drawn into confrontations with potentially

dangerous taxpayers. Congress decided to require IRS to drop the ITP designation over concerns that the label could bias IRS employees and result in unfair treatment of the taxpayer.

While the ITP designation was abolished, RRA 98 did provide IRS the authority to implement additional procedures, such as the maintenance of appropriate records, in connection with this provision so as to ensure IRS employees' safety.

NTEU believes it is critical that IRS ensure that any and all information relevant to employees' safety will always be available to them.

LEO Status for Revenue Officers

NTEU is very concerned about the level of threats and violence against IRS employees, and in particular, against Revenue Officers (ROs), who often must meet with taxpayers on a one-on-one basis in the course of conducting their investigations.

According to the IRS, between 2003 and 2007, RO's reported more than 480 cases involving Potentially Dangerous Taxpayers (PDTs), a designation assigned to taxpayers who have demonstrated a capacity for violence against employees of the IRS, contractors or their families, and Caution Upon Contacts (CAUs), defined as those incidents that posed a less immediate and less serious threat.

This report comes at a time when the threat of violence against Federal employees is receiving increased attention and anti-government sentiment remains at an all-time high.

But despite these startling figures, ROs are not authorized to carry and or use firearms in performance of their official duties and are forced to request assignment of an armed escort to ensure their own safety. According to TIGTA, it expects the necessity for armed escorts to increase over time as the IRS places additional focus on collection and enforcement activity.

NTEU strongly believes that the high number of threats and assaults recently reported by TIGTA once again illustrates the clear need for RO's to be granted LEO status. That is why NTEU strongly supports legislation currently pending in the subcommittee, H.R. 673, the "Law Enforcement Officers Equity Act," which would grant law enforcement retirement benefits to ROs at the IRS. These officers face dangerous situations as they enforce the United States Tax Code and collect delinquent taxes. Most people see these individuals as law enforcement officers, and many have reacted to their inquiries with threats, assaults, and in some cases gunfire. Yet, these men and women are being denied the rights and benefits of their colleagues who are considered to be law enforcement officers.

While some in the government have expressed concern that legislation providing coverage for these officers would have a negative impact on personnel costs for government agencies, this argument is fundamentally flawed. Granting LEO status to ROs will actually decrease personnel costs by increasing morale and officer retention, thus decreasing the costs associated with training new officers.

NTEU asks for the committee's support for this critical legislation that will enhance the safety and security of Revenue Officers as they carry out their tax enforcement mission.

Anti-Government Rhetoric

Mr. Chairman, each and every day, Federal employees, such as those at the IRS, who have dedicated their lives to serving others, work under the constant threat of attack due the nature of their work. But despite this, these dedicated employees continue to carry out their duties on behalf of the country.

Yet, far too often, federal employees, and the good work that they do, are portrayed in an unfavorable light. In particular, in the aftermath of the Austin tragedy, I have been shocked to hear a number of comments from politicians and commentators alike expressing empathy for the man responsible for the cowardly actions that took the life of a dedicated public servant, or somehow trying to justify the man's actions by blaming government workers. Make no mistake, offensive and irresponsible comments such as these that denigrate the good work of federal employees are inexcusable and are precisely the kind of irresponsible rhetoric that can turn frustration with policies and politics into attacks on public servants and can contribute to misguided rage against federal workers and threaten their safety.

That is why in 2008, in an effort to dispel negative stereotypes and increase awareness of the important contributions federal employees make to the country, NTEU launched a public service campaign including television and radio public service announcements, media relations, and grassroots efforts.

The campaign, entitled "Federal Employees...They Work For U.S.," features actual federal workers talking about the work that they do to defend our homeland, protect our borders, ensure the safety of our natural resources, health, food supply, financial systems, and more.

Mr. Chairman, NTEU believes it is well past time that we began focusing on the excellent work federal employees do for our country and their dedication to duty, rather than using them as scapegoats for problems not of their making. We believe public service is a high and honorable calling and that we are fortunate to have a committed, dedicated and talented workforce serving our government at this hour of our nation's need. We believe all federal employees deserve a secure environment while doing the nation's work and stand ready to work with Congress and the Administration to do whatever is necessary to ensure their safety.

I truly appreciate the efforts of many public officials, including Congressman Lloyd Doggett of Texas who authored H.Res.1127 to express the House of Representatives' support for the IRS workers who were attacked in Austin and President Obama who sent a letter to me, denouncing the actions of the Austin suicide attacker and pledging to ensure the safety of federal employees.

I also very much appreciate the Subcommittee holding this hearing today. Federal workers need to know that their elected representatives appreciate their service and will do what needs to be done to protect them.

Thank you.

Mr. LYNCH. Thank you.

Mr. Adler, you are now recognized for 5 minutes.

STATEMENT OF JON ADLER

Mr. ADLER. Thank you. Chairman Lynch, Ranking Member Chaffetz, and distinguished members of the committee, on behalf of the 26,000 membership of the Federal Law Enforcement Officers Association, I thank you for the opportunity to appear before you today.

My name is Jon Adler and I am the National President of FLEOA. I am proud to represent Federal law enforcement officers from over 65 different agencies, including FPS, IRS criminal investigation, Treasury IG, Postal Inspection, and Secret Service. My statement includes specific comments from members from these agencies, as well as others.

In the course of my 19 years in Federal law enforcement, I served as a first responder at Ground Zero on September 11, 2001, and in New Orleans after Hurricane Katrina hit. From these two catastrophic events, I witnessed the devastation terrorism and acts of nature can have on the safety and security in a Government workplace. From these horrific events, there was a lot to be learned. It is our collective responsibility to apply this knowledge and not let it rest like an old gun trapped in an unworn holster.

We can learn a lot from the feedback I received from seasoned law enforcement officers employed by a diverse group of agencies. Their comments reflect both the employee and protective perspective. Here are some examples: Regarding GSA, GSA had a program they called first impressions where they attempted to blend security screening into the aesthetics of the building. This pushed back the security screening from the immediate area of the entry to the facility into the building lobby. The Israeli security procedure is to identify the threat before it reaches and enters the protected facility. All new security screening stations need to be constructed and existing ones retrofitted with the protection of the security officers in mind.

Regarding IRS, IRS employees work in GSA-owned or leased space which FPS has statutory authority to protect, which includes uniformed law enforcement response and criminal investigations. IRS agencies do not pass any information along to FPS regarding persons who have threatened an IRS facility or employee. Their withholding of threat information puts the facilities, their employees, and any citizen in the facility at risk. IRS has not prepared their special agents for responding to situations such as what happened in Vegas or Austin.

Frankly, with all the training IRS employees receive, it is shameful that IRS has not implemented a workable plan to respond to incidents like the one in Austin. I believe it is time for IRS criminal investigation to create a program or training course that addresses terrorist type attacks against IRS. The fact that IRS is unwilling to refer to violent tax evaders as tax protesters shows their lack of commitment to workplace threats.

Regarding the Postal Service, I watched automatic lawn sprinkling equipment installed while denied request for less than $5,000 worth of security improvements in the same facility. I have wit-

nessed longstanding security specifications minimized or outright eliminated for perimeter facing, investigative observation, robbery countermeasures, vehicle breaking countermeasures, etc., where, if the Inspection Service is even consulted, the decision is pre-ordained to lower or eliminate the existing standards. There are post offices in desperate need of bullet-resistant screen lines but go unfunded due to their cost.

Regarding courthouse and probation, there are six judicial districts where the chief judges will not allow qualified probation and pretrial officers to be armed and defend themselves in the work force. It is mind boggling that we have officers go through 40 hours of firearms training and not be allowed to carry a firearm. It is not uncommon for offenders and their associates to loiter outside public buildings before or after meetings or interviews with officers, and this poses a risk for the officers, the workers, and the community.

Several Federal courthouses have no security presence after hours on weekends or holidays. Employees' only protection is their access card and their PIN. It is a total joke. The bottom line is, without a security presence the officers and their employees are vulnerable to an attack.

FLEOA member recommendations include: FPS is available to assist in GSA-owned and leased space with occupant emergency planning and exercises and active planning and awareness training, which I believe Director Schenkel hit on.

The Secret Service uses a continuity of operations plan in all of its offices to address emergency response, evacuation routes, relocation, and contact information. Each office is equipped with emergency equipment, and every employee is given a co-op card with pertinent emergency information. Other agencies may benefit from adopting all or some of this system. Each agency should run unannounced security tests aimed at improving layers of protection and not punishing those who don't succeed.

Set up an interagency task force with experienced law enforcement officers to address building and equipment vulnerabilities, threat assessment, and response protocols, threat information sharing, and human capital needs.

Agency heads should provide Congress with a list of their security needs to ensure funding for appropriate staffing levels, training, and functional security equipment. In turn, each agency head must commit to spending funds for specific security needs, with the expectation of enhanced security measures, the general Government employee audience must embrace the implementation of new technology such as the advanced imaging technology now being used by TSA.

In closing, I will offer that the best playbook or operational plan accomplishes nothing when it is layered with dust. All agencies should practice emergency response protocols and periodically test their defense systems. With the appropriate level of funding, agency staffing, equipment, and training needs will be met. It is imperative that the agency have the means to take proactive measures to improve workplace security and emergency response capabilities.

We all need to claim ownership of this challenge, and we all need to commit to its success.

Thank you, Mr. Chairman.

[The prepared statement of Mr. Adler follows:]

FEDERAL LAW ENFORCEMENT OFFICERS ASSOCIATION
P.O. Box 326 Lewisberry, PA 17339
www.fleoa.org
(717) 938-2300

Representing Members Of:
AGENCY for INTERNATIOANAL DEVELOPMENT
AGRICULTURE-OIG and FOREST SERVICE
COMMERCE
Export Enforcement, OIG
& NOAA Fisheries Law Enforcement
DEFENSE
Air Force - OIG
Army - CID
Defense Criminal Investigative Service
Naval Criminal Investigative Service
OIG
EDUCATION - OIG
ENERGY -OIG
ENVIRONMENTAL PROTECTION AGENCY - CID & OIG
FEDERAL DEPOSIT INSURANCE CORPORATION - OIG
GENERAL SERVICES ADMIN -OIG
HEALTH & HUMAN SERVICES
Food & Drug Administration & OIG
HOMELAND SECURITY
Border Patrol
Coast Guard Investigative Service
Immigration & Customs Enforcement
Federal Air Marshal
Federal Emergency Management Agency
Federal Protective Service
US Secret Service
Transportation Security Administration
HOUSING & URBAN DEVELOPMENT - OIG
INTERIOR
Bureau of Indian Affairs
Bureau of Land Management
Fish & Wildlife Service
National Park Service
OIG
U.S. Park Police
JUSTICE
Bureau of Alcohol, Tobacco, Firearms & Explosives
Drug Enforcement Administration
Federal Bureau of Investigation
US Marshals Service
OIG
U.S. Attorney's Office-CI
LABOR- OIG & Racketeering
NATIONAL AERONAUTICS & SPACE ADMIN - OIG
NUCLEAR REGULATORY COMMISSION - OIG
POSTAL SERVICE-OIG & Inspection
RAILROAD RETIREMENT BOARD - OIG
SECURITIES & EXCHANGE COMMISSION - OIG
SMALL BUSINESS ADMINISTRATION - OIG
SOCIAL SECURITY ADMINISTRATION - OIG
STATE DEPARTMENT
Bureau of Diplomatic Security & OIG
TRANSPORTATION-OIG
TREASURY
FINCEN & OIG
Internal Revenue Service - CI
TIGTA
U.S. COURTS (JUDICIAL)
Probation, Parole & Pretrial Services
VETERANS AFFAIRS -OIG

NATIONAL OFFICERS
President
JON ADLER
Executive Vice-President
NATHAN CATURA
Vice President - Operations
LAZARO COSME
Vice President - Agency Affairs
CHRIS SCHOPPMEYER
Vice President - Membership Benefits
JOHN RAMSEY
Secretary
MARIA COSCIA
Treasurer
JAMES OTTEN JR
Legislative Director
DUNCAN TEMPLETON
National Chapters Director
RASHEED LAHIR
National Awards Director
SHANON MAST-MCPHERSON
Legislative Consultants
MCALLISTER & QUINN
ANDY QUINN
Legislative Counsel
[illegible]

March 16, 2010

House Subcommittee on Federal Workforce, Postal Service and the District of Columbia Hearing

Chairman: The Honorable Stephen F. Lynch
Ranking Member: The Honorable Jason Chaffetz

Hearing: "Examining Federal Employee Workplace Safety and Security."

Federal Law Enforcement Officers Association
Witness Statement: Jon Adler, National President

Chairman Lynch, Ranking Member Chaffetz, and Distinguished Members of the committee, on behalf of the 26,000 membership of the Federal Law Enforcement Officers Association (FLEOA), I thank you for the opportunity to appear before you today. My name is Jon Adler and I am the National President of F.L.E.O.A. I am proud to represent federal law enforcement officers from over 65 different agencies, including FPS, IRS-CID, TIGTA, PIS, and the USSS. My statement includes specific comments from members from these agencies, as well as others.

In the course of my 19 years in federal law enforcement, I served as a first responder at Ground Zero on September 11, 2001, and in New Orleans after Hurricane Katrina hit. From these two catastrophic events, I witnessed the devastation terrorism and acts of nature can have on the safety and security in the government workplace. From these horrific events, there was a lot to be learned. It is our collective responsibility to apply this knowledge, and not let it rust like an old gun trapped in an unworn holster.

We can learn a lot from the feedback I received from seasoned law enforcement officers employed by a diverse group of agencies. Their comments reflect both

the employee and protector perspective. Here are some examples:

"GSA had a program they called "First Impressions" where they attempted to blend the security screening into the aesthetics of the building. This pushed back the security screening from the immediate area of the entrance of the facility into the building lobby. The Israelis' security procedure is to identify the threat before it reaches and enters the protected facility. All new security screening stations need to be constructed (and existing ones retrofitted) with the protection of the security officers in mind."

"IRS employees work in GSA owned or leased space which FPS has statutory authority to protect, which includes uniformed law enforcement response and criminal investigations. IRS agencies do not pass any information along to FPS regarding persons who have threatened an IRS facility or employee. Their withholding of threat information puts the facilities, their employees and any citizen in the facility at risk."

"IRS has not prepared their Special Agents for situations such as what happened in Vegas or Austin. Frankly, with all the training IRS employees receive, it's shameful that IRS has not implemented a workable plan to respond to incidents like the one in Austin. I believe it's time for IRS-CID to create a program or training course that addresses terrorist type attacks against IRS. The fact that the IRS is unwilling to refer to violent tax evaders as "tax protesters" shows their lack of commitment to workplace threats."

"Postal Service: I watched automatic lawn sprinkling equipment installed while denied requests for less than $5000 worth of security improvements on the same facility. I have witnessed long-standing security specifications minimized or outright eliminated for perimeter fencing, investigative observation and robbery countermeasures, vehicle break-in countermeasures, etc, where if the Inspection Service is even consulted the decision is preordained to lower/eliminate the existing standards. There are post offices in desperate need of bullet resistant screen lines, but go unfunded due to their cost."

"Courthouse/Probation: There are six judicial districts where the chief judges will not allow qualified Probation and Pretrial Officers to be armed and defend themselves and the workforce. It is mind boggling that we have new Officers go through 40 hours of firearms training and not be allowed to carry a firearm. It is not uncommon for Offenders and their associates to loiter outside public buildings before or after meetings/interviews with Officers, and this poses a risk to the Officers, office workers and the community."

"Several federal courthouses have no security presence after hours, on weekends and holidays. Employees' only protection is their access card and PIN – it's a total joke. The bottom line is without a security presence, the offices and their employees are vulnerable to an attack."

FLEOA Member Recommendations include:

"FPS is available to assist agencies in GSA owned/leased space with Occupant Emergency Planning and Exercises, and Active Shooter Plans with Awareness Training."

"The Secret Service uses a Continuity of Operations Plan (COOP) in all of its offices to address emergency response, evacuation routes, relocation and contact information. Each office is equipped with emergency equipment and every employee is given a COOP card with pertinent emergency information. Other agencies may benefit from adapting some or all of this system."

"Each agency should run unannounced security tests aimed at improving layers of protection and not punishing those who don't succeed."

"Set up an interagency task force with experienced law enforcement officers to address building and equipment vulnerabilities, threat assessment and response protocols, threat information sharing, and human capital needs."

"Agency heads should provide Congress with a list of their security needs to ensure funding for appropriate staffing levels, training and functional security equipment. In turn, each agency head must commit to spending funds for specific security needs. With the expectation of enhanced security measures, the general government employee audience must embrace the implementation of new technology, i.e., Advanced Imaging Technology."

In closing, I will offer that the best play book or operational plan accomplishes nothing when it's layered with dust. All agencies should practice emergency response protocols, and periodically test their defense systems. With the appropriate level of funding, agency staffing, equipment and training needs will be met. It is imperative that agencies have the means to take proactive measures to improve workplace security and emergency response capabilities. We all need to claim ownership to this challenge, and we all need to commit to its success.

Respectfully submitted,

Jon Adler

Jon Adler

Mr. LYNCH. Thank you, Mr. Adler.

Mr. Wright, you are now recognized for 5 minutes.

STATEMENT OF DAVID WRIGHT

Mr. WRIGHT. Mr. Chairman, Ranking Member Chaffetz, and members of the subcommittee, Mr. Chairman, as president of the FPS Union, it has never given me pleasure to bring attention to this crisis. Indeed, I have dedicated the last 24 years of my life trying to make this agency the best law enforcement Homeland Security agency in the country, but when our members see every day how serious the problems are, I am obligated to speak out.

Over the past 2 years, the Federal Protective Service has been investigated, analyzed, and studied. The GAO has performed six studies since 2008 addressing different aspects of FPS, and all concluded that the agency is rife with serious problems, each of which is impairing the ability of FPS to perform its critical homeland security mission. Taken together, the GAO analyses paint a portrait of an essentially dysfunctional agency.

The mission of the FPS is to protect approximately 9,000 high, medium and low-security Federal buildings and properties around the country. These buildings include everything from Social Security offices, Federal courthouses, Federal congressional offices, and agency headquarters. Hundreds of thousands of Federal employees work in these buildings, and millions of Americans visit every day.

Time and again, Federal buildings and employees have been demonstrated to be targets. Recent events in Washington, DC, Austin, Las Vegas, and even Kansas City serve as a wake-up call to both the administration and Congress that the time for discussion, studies, years of reports that highlight the same failures has ended. Action is required now, and not after the next major terrorist attack.

Regarding manpower, in the period following the terrorist attack on the Alfred P. Murrah Federal Building in Oklahoma City, it was determined that the minimum number of FPS personnel necessary to perform its mission was 1,480. Since the Department of Homeland Security was stood up in 2003, the FPS has seen its total number of inspector and police officer positions drop from 1,017 in 2003 to 830 at the beginning of 2010, an 18.4 percent reduction.

Over the same period, U.S. Parks Service increased its security personnel by 45.5 percent. The Veterans Health Administration increased its security personnel over 35.9 percent. Even within DHS, security personnel increased over the 7-year period of 230.5 percent. The result of this resource starvation is that FPS security services have been slashed to the point of ineffectiveness. No longer do FPS police officers operate on a 24-hour patrol basis, even when responsible for protecting level four high-security facilities. No longer does the agency have the personnel necessary to adequately oversee private guards due to a lack of manpower.

All of this has occurred in a post-9/11 environment that has made anti-terrorism efforts the highest of priorities in the White House and Congress. As a result of the extremely limited resources provided to FPS, the agency has been in disarray, leaving employees in certain of their jobs, contract guards, routinely unsupervised,

and managers operating fiefdoms free of any central control of direction.

Mr. Chairman, I believe we are on borrowed time when it comes to this very large gap in our national homeland security safety net.

Contract guard issues, every day Federal protective officers put their lives on the line to accomplish their critical homeland security mission, to make sure facilities are protected and contract guards are correctly trained and proficient in their duties. Despite these efforts, FPS does not have sufficient staff to accomplish these vital tasks.

One glaring example is the monitoring and training of contract guards. In 2001, there were 5,000 contract guards and FPS was authorized over 1,450 personnel. By 2009, there were 15,000 contract guards, but FPS was authorized only 1,225 total personnel. A threefold increase in guards coupled with a 16 percent cut in FPS staff is a recipe for failure.

No one should have been surprised to discover shortfalls in contract guard management, performance, and ability to detect weapons and explosives. Clearly, OMB should have increased the resources for monitoring rather than imposing a cut.

In conclusion, I would like to thank the members of the committee for holding this hearing. I hope that it will serve as the beginning of a process that will lead to comprehensive FPS reform legislation this year. I know that Senator Lieberman has announced his intention to introduce such legislation soon, and we urge the House to do so, as well.

Thank you.

[The prepared statement of Mr. Wright follows:]

STATEMENT OF DAVID L. WRIGHT,

PRESIDENT

LOCAL 918 – FEDERAL PROTECTIVE SERVICE

AMERICAN FEDERATION OF GOVERNMENT EMPLOYEES

BEFORE THE

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

SUBCOMMITEE ON THE FEDERAL WORKFORCE, POSTAL SERVICE AND DISTRICT OF COLUMBIA

U.S. HOUSE OF REPRESENTATIVES

HEARING ON

"Federal Employee Workplace Security"

March 16, 2010

Mr. Chairman, Ranking Member Chaffetz and Members of the Subcommittee:

My name is David Wright and I am the President of the Federal Protective Service Union. I am testifying today, not only on behalf of our members at FPS, but also on behalf of the American Federation of Government Employees.

Introduction:

Over the past two years, the Federal Protective Service has been investigated, analyzed and studied. The GAO has performed six studies since 2008 addressing different aspects of FPS, but all concluded that the agency is rife with serious problems, each of which is impairing the ability of FPS to perform its critical homeland security mission. Taken together, the GAO analyses paint a portrait of an essentially dysfunctional agency.

Mr. Chairman, as President of the FPS Union, it has never given me pleasure to bring attention to this crisis. Indeed, I have dedicated the last 20 years of my life, trying to make this agency the best law enforcement/homeland security agency in the country. But when our members see every day how serious the problems are, they urge me to speak out.

The mission of the FPS is to protect approximately 9000 high, medium and low security federal buildings and properties around the country. These buildings include Social Security offices, federal facilities housing Members of Congress and other Federal officials, Level Four high security facilities and others. Hundreds of thousands of federal employees work in these buildings and millions of Americans visit them every day.

Time and again, federal buildings and employees have demonstrated themselves to be targets. Recent events in Washington DC, Austin, Las Vegas and Kansas City serve as a wakeup call to both the Administration and Congress that the time for discussion, studies and years of reports that highlight the same resource failures has ended; action is required now not after the next major terrorist attack.

Manpower: (Post September 11, 2001)

In the period following the terrorist attack on the Alfred P. Murrah building in Oklahoma City, it was determined that the minimum number of FPS personnel necessary to perform its mission was 1480. FPS has never reached that level of personnel. Since the Department of Homeland Security was stood up in 2003, the Federal Protective Service has seen its total number of Inspector and police officer positions drop from 1,017 in that year to 830 at the beginning of

2010 – an 18.4 percent reduction. Over the same period, the U.S. Park Service increased its security personnel by 45.5% or 260 FTE's. The Veterans Health Administration increase in security personnel numbered 820 for 35.9%. Within DHS, security personnel increased from 59 to 195 over the seven year period or 230.5 %. **

In fact, the situation is so bad that even current staff levels are below congressionally mandated levels. The FY 10 DHS Appropriations Act mandates that OMB and DHS shall ensure fee collections are sufficient to ensure that the Federal Protective Service maintains not fewer than 1,200 full-time equivalent staff and 900 full-time equivalent Police Officers, Inspectors, Area Commanders, and Special Agents who, while working, are directly engaged on a daily basis protecting and enforcing laws at Federal buildings (referred to as `in-service field staff'). Based on ICE and OMB guidance the FPS in-service field staff has been interpreted as including all personnel assigned to FPS law enforcement positions. Thus the 900 minimum includes recruits who have not even attended FLETC Uniformed Police training, personnel on long term restricted duty that prevents service as a law enforcement officer.

The result of this resource starvation strategy, largely conducted by the Office of Management and Budget, is that FPS security services have been slashed to the point of ineffectiveness. No longer do FPS police officers operate on a 24 hour patrol basis – even when protecting level IV high security facilities; no longer does the agency have the personnel necessary to adequately oversee private guards and no longer is FPS able to adequately monitor the state of security equipment at federal buildings -- due to a lack of manpower.

All of this has occurred in a Post 9/11 environment that has made anti-terrorism efforts the highest of priorities in the White House and Congress. As a result of the extremely limited resources provided to FPS, the agency has been in disarray leaving employees uncertain of their jobs, contract guards routinely unsupervised and managers operating fiefdoms free of any central control or direction. Mr. Chairman, I believe we are on borrowed time when it comes to this very large gap in our national homeland security safety net -- and that time is running out.

Contract Guard Issues:

Every day, Federal Protective Service officers put their lives on the line to accomplish their critical homeland security mission and have willingly sacrificed their leisure and family time to work the many hours of overtime required to make sure facilities are protected and contract guards are correctly trained and proficient in their duties. Despite these yeoman efforts, FPS does not have sufficient staff to accomplish these vital tasks. While we are finally confident the Department leadership wants FPS to succeed, we need your help to make sure the embedded,

intransigent and unaccountable bureaucrats at OMB cooperate to provide the minimum resources necessary to accomplish our mission.

One glaring example is the monitoring and training of contract guards. In 2001 there were 5,000 contract guards and FPS was authorized over 1,450 total personnel. By 2009 there were 15,000 contract guards, but FPS was authorized only 1,225 total personnel. A three-fold increase in guards coupled with a 16% cut in FPS staff was a recipe for failure. No one should have been surprised to discover shortfalls in contract guard management, performance and ability to detect weapons and explosives. Clearly OMB should have increased the resources available for monitoring, rather than imposing a cut.

Based in the GAO test, where without detection, their investigators entered facilities with bomb –making materials; the overreliance on contract guards – particularly at the highest security level buildings – has clearly reduced the effectiveness of security provided around these facilities. The staggering lapses found by the GAO make insourcing of contract guards at high risk buildings an important component of any overall reform effort for FPS.

FPS Management Issues:

FPS can better manage its mission as the GAO has highlighted management in many regions have been deficient - there is simply no excuse for not monitoring required guard certifications or developing and implementing a workable Human Capital Strategy.

The overdue transfer of FPS to NPPD has occurred and the employees of FPS look forward to the recognition and correction of the many management failures noted by the GAO. It remains essential that those selected for management roles have real and substantial experience with community policing strategies to deliver both law enforcement and security services to properly protect Federal workplaces. All too often our front line officers are mystified at the 'whack a mole' nature of policy changes made with no real input from the limited cadre of employees with field law enforcement experience.

Congress needs to consider a significant increase in the number of Series 0080 FPS Police Officers as a way of restoring the agencies' ability to adequately perform contract oversight. Such an increase would also allow FPS to provide better security for all FPS protected buildings by enabling 24 hour community patrolling and vastly improved oversight of building security equipment.

FPS Structural Problems

In the Homeland Security Act, the DHS Secretary was charged with the responsibility to protect Federal facilities and employees in their workplaces. Instead of increasing staff and budgetary authority to meet this mandate cuts were proposed with the intent of creating an unfunded mandate on the agencies the Department was created to protect. The very way Federal security standards are set and implemented is dysfunctional; driven by ad hoc committees that must attempt to establish and implement security standards on a consensus basis, where any funding for essential security must come from agency funds at the expense of their statutory mission. The result is often inaction, diminished security and increased risk to employees. Now is the time for DHS to step up and accomplish it critical Federal workplace protection mission. Serious steps are required to right this floundering ship and restore a correct course:

- Change the existing funding scheme that forces agencies to choose between funds for their daily mission and protecting their employees. Appropriate the funding required to secure Federal facilities and protect the dedicated civil servants who work in them to DHS. .
- Firmly place DHS in charge of determining standards and requesting the finding necessary to implement them. Advice and counsel from supported agencies is essential but current year funding availability simply cannot be the only driver determining compliance with a standard.
- Clearly establish DHS FPS as the lead for coordinating threats, informing local law enforcement and jointly investigating threats with agency investigators (such as TIGTA). Only an integrated approach will allow the dots to get connected. The current fragmented approach is a failure point waiting to happen.
- Increase the staffing of the FPS to provide agencies with regular emergency planning assistance and practice of each element of the plan including coordination with local authorities and facilities.
- FPS staffing must also be sufficient to conduct the proactive police patrol activities GAO found essential to detect and deter attacks. Terrorists, nuts and criminals don't work bankers hours and neither should FPS, yet 24-hour service is only provided in two cities. At a minimum, around the clock protection by Federal Law Enforcement Officers should be provided in the 18 to 22 cities with the greatest concentration of employees and facilities.

In addition to these recommendations, the FPS union urges Congress to support work place improvements for those employees who remain committed to the work and mission of the Federal Protective Service. This can easily be accomplished by providing law enforcement retirement benefits to those FPS employees still young enough to apply for them and to grant

them the same power every other law enforcement officer has to carry his or her service weapon on a 24-hour basis. Taken together these measures, which would cost less than $10 million, offer the best hope of restoring the morale of workers at this once proud federal security agency.

Conclusion:

In conclusion, I would like to thank the Members of this Committee for holding this hearing. I hope that it will serve as the beginning of a process that will lead to comprehensive FPS reform legislation this year. I know that Senator Lieberman has announced his intention to introduce such legislation soon and we urge the House to do so as well. Thank you.

** See below

Benchmarks for comparison of the Federal Protective Service

FY 03 (Transfer to DHS) with FY 2010

The Federal Protective Service did not have sufficient staff to effectively accomplish its GSA facilities protection mission when it was transferred to DHS.

- Post Murrah bombing required FTE was 1,480.
- 1,456 FTE were transferred to DHS.
- Necessary overhead increases (i.e. contracting) are at expense of the field force.
- Staffing shortages exist for:
    - effective monitoring above the 5,000 contract guard level;
    - proactive patrol;
    - countermeasure verification (i.e. tenants expected to test own alarms); and
    - facility security officer role to assist security committees.

Most of the law enforcement and security roles of the FPS are accomplished by staff in series 0083 and 0080. Since 2003 there has been exponential growth of security and law enforcement staff in virtually every agency, except FPS.

The below table compares the civilian workforce in these two series for FY 2003 and FY 2010 in comparable security and law enforcement organizations and government wide:

U.S. and Territories Only	Total On Board series 0083 and 0080			
Agency	**FY 2003**	**Beginning FY 2010**	**Increase**	**Percent Increase**
Government Wide	16,240	25,422	9,182	56.5%
FPS	**1,017**	**830**	-187	-18.4%
Secret Service (Police and Security)	1,213	1,511	298	24.6%
Park Service	571	831	260	45.5%
Veterans Health Administration	2,287	3,107	820	35.9%
FBI	443	906	463	104.5%
FEMA	72	140	68	94.4%

DOD	7,997	14,013	6,016	75.2%
Gov't Wide Excluding DOD	8,243	11,409	3,166	38.4%

*FPS FY 2003 is the number of positions in series 0083 and 0080 transferred from GSA to DHS.

**Capitol Police was not included as a potential benchmark because personnel data is not available from OPM's database.

The table below shows increases of in-house government security specialists (series 0080) for some FPS customer agencies, including GSA:

Agency	FY2003	FY 2010	Increase	Percent Increase
SSA	41	78	37	90.2%
CBP	59	195	136	230.5%
CIS	42	99	57	135.7%
ICE	25	89	64	256.0%
EPA	13	25	12	92.3%
GSA	4	31	27	675.0%

Since 2003 the number of facilities FPS protects has increased by over 1,200 buildings. The most dramatic change is the number and complexity of guard posts and countermeasures. No longer can we depend on a guard with 8 hours of x-ray training to find a knife or an assembled pipe bomb using a magnetometer and x-ray. As GAO clearly pointed out, the guards must be trained, tested and coached to be able to identify and prevent entry of all explosive and weapons components. The FPS field force simply does not have enough Police Officers and Inspectors to properly accomplish its mission.

The below table illustrates the number of guards requiring supervision, monitoring, evaluation and training from FPS:

	# of Guards	Guards per FPS Officer
FY 2001	5,000	6.3

FY 2003	7,000	8.1
FY 2010	15,000	18.3

FPS officer includes in-service field staff in series 0083 and 0080.

The below table illustrates differences in average buildings per Officer, the decrease in service and decrease in arrests between 2003 and 2010. The decrease in arrests is attributed to the virtual elimination of proactive patrol and curtailed service hours – the offenses still happen but the perpetrator is not caught.

	2003	2010
Buildings per Inspector/ Police Officer	7.7	11.0
GSA Managed Sq Ft per Officer	322K	426K
Cities with Night and Weekend Service	12	2
Arrests by Officers/ Inspectors (Lack of patrol results in fewer arrests)	3100	1600

Below is the number of additional FPS series 0080 and 0083 positions that would be required if that agency 2003 to 2009 increase was used as a benchmark:

	Rate of Increase 2003 to 2010	Increase required to match rate
Increase at DOD rate	75.2%	765
Increase at Gov't wide rate	56.5%	575
Increase at Park Svc rate	45.5%	463
Increase at VA rate	35.9%	365
Increase at Gov't wide except DOD rate	38.4%	391

Observations

An increase of 391 FPS in-service law enforcement staff would match the increase in like positions for non-DOD agencies between FY 2003 and FY 2009. That would reduce number of guards per Officer to 12.4 from 18.3. A rough estimate of the total funding required would be $75M after the first year. If the guard contract administrative charge was restored to the FY 09 level of 8% the first year increase in basic security charges would only be 7 to 8 cents. An alternative would be a one year stop-gap appropriation of $48M to allow programming of the increased security charge within the budget cycle.

While searching for benchmarks it was observed that while there is an "object class" for what agencies pay in GSA rent there is no equivalent measure for facilities security expenditures which could have been used as a benchmark for this exercise.

Mr. LYNCH. Thank you, Mr. Wright.

I now yield myself 5 minutes.

President Kelley, you had an opportunity to go to the IRS facility in Austin. You had a chance to talk to the employees. First of all, my condolences to your organization for that loss.

Ms. KELLEY. Thank you.

Mr. LYNCH. What were the suggestions, recommendations, urgings that you heard there in terms of trying to address that situation on the ground? Were there any concrete recommendations that came out of at least a preliminary investigation?

Ms. KELLEY. In the immediate aftermath, Mr. Chairman, there really have not been. The focus has been more on what happened that day and how so many were able to get out successfully. For example, when we were there and met with the employees, they thanked their co-worker who had been responsible for fire drills. And everybody knows whoever runs the fire drills, somebody is always trying to hide to not have to actually practice. And they made it a point of thanking her, because they knew what to do that day.

So there really has been more thought to now getting them situated. They just returned to work last Monday in other buildings until there is a new replacement building for them to move to.

So now the conversations are more leaning toward what can be done, you know, what are they concerned about, what should we pay attention to for the future, especially in the new site that they will be moving to. So as that develops, we will be working very closely with the IRS in an effort to put plans in place that make those suggestions reality.

Mr. LYNCH. Thank you.

We are sort of doing an informal assessment across the board for IRS facilities, and I notice that there are—and I am not sure which level. I know you have different levels of sensitivity and security that are required. But I did notice that there were about 275 facilities that had no protection whatsoever, not even security guards.

I am just curious, you know, each of you, what your thoughts are on that. I think that might be a function of this 1,250 minimum staffing requirement, that you just don't have enough folks. I know there is also an additional 15,000 private security guards that are hired as contractors to do some of the, I guess, basic security outside the building, that type of thing. Your thoughts on the manning requirement and also the status of having at least 275 IRS facilities that don't have any security whatsoever.

Ms. KELLEY. I will say for my part that employees would say there are too many IRS facilities without some guard presence. I am sure that Mr. Wright knows better than I the number that have FPS presence. Most of them that I am aware of, some of the larger buildings have FPS, but the majority of them have contract guards rather than FPS.

Like I said, this is an issue for employees. Many of them believe their facility and the situation that they are in warrants a guard. It comes down to resources. It is an issue we are always debating the IRS with over the money, because there is a cost attached to it, definitely. But it is an issue that has been long a point of disagreement between us over how much is needed.

Obviously, as someone had asked before, the Austin attack was not going to be prevented by having guards or FPS there, but it highlights, when things like that happen it makes you think about the things that can be controlled and the need for a focus and a recognition that there need to be resources to adequately protect these buildings.

Mr. LYNCH. Mr. Adler, same question.

Mr. ADLER. Yes. I agree. Colleen is exactly right. It is a resource issue. And in this instance, it is a matter of response. If you don't have a physical presence, if you put 2 people on a playing field to go against an 11 with a full bench, as well, you can't play. You are at a tremendous disadvantage and people are at risk.

So what do you do? I think one of the disputes, I represent IRS special agents as well as TIG, or Treasury IG special agents, and they have a little ongoing dispute as to who responds to certain situations. So if you don't have perimeter or building security but in certain instances you may have special agents in there, well, guess what, they are responsible and they own it and they need to be trained to respond. They can't have any doubt. You can't play who is in charge when it hits the fan.

One of the issues that needs to get addressed and needs to be resolved is who claims ownership and what training is in play to respond.

Colleen is absolutely right: we are not concerned, well, we can't prevent a plane. That is beyond our Superman and Superwoman abilities. You can't prevent a plane from flying into a building. But what happens in a situation like what happened in the Las Vegas courthouse, only now it is an IRS facility? And instead of one elderly person with mental issues coming in with a shotgun, you have more highly skilled, trained terrorists coming in with assault weapons? Well, what do we do? We should have an answer. We can't make this up when it happens. We need to get it done and planned for now.

Mr. LYNCH. Thank you.

Mr. Wright.

Mr. WRIGHT. Yes, sir, this kind of delves back into the ISC and the facilities security committees. The ISC is not codified. They are not the authority. They come up with recommendations, and once those recommendations reach the field it is up to an FPS inspector, when we are dealing with our buildings, our properties that we are responsible for, it is up to that inspector to take those recommendations, make those recommendations to the facilities security committee, which is mainly staffed by lay personnel. Very rare that you get a good security-wise person on those committees.

So what happens, the reason you would have a number of properties, IRS properties that have no security personnel onsite is the recommendations have likely been made, they have been presented to the Facility Security Committee. That committee has to weigh that recommendation against their yearly budget, usually their operating budget. Sometimes they have security funds, sometimes they don't. Generally, these things get voted down. There is no authority at this time to mandate any building in any sector of the Government to provide security.

I know of a case now of a very major Federal building where a GSA type is the head of the Security Committee and you would be very surprised how lacking that is. I would be glad to tell you about it behind closed doors, because it just does not happen.

Mr. LYNCH. All right. Thank you very much.

I now yield 5 minutes to the ranking member, Mr. Chaffetz.

Mr. CHAFFETZ. Thank you.

Ms. Kelley, there are many great acts of heroism that happened in Texas, and for that we are eternally grateful and thankful. I am sure we will never hear all of the stories of people who reacted the right way at the right time and woke up that morning and had no idea that was going to happen, so for that we are so grateful, and obviously saddened for the loss of anybody who should never have had to go through that, nor should their family. It is just absolutely and totally inexcusable.

It is still early, but, based on what you have known or have seen or have heard, at least at this point, what is it in Texas that could have or should have happened that maybe didn't happen, because the results were in many ways miraculous, but at the same time there is always things you want to learn and share and grow from. So can you give us a little insight as to that perspective?

Ms. KELLEY. No. Again, the focus has been on whether it was the luck or just everyone acting together, just the pulling together. I mean, I really have not heard of anything that day someone said I wish this or I wish that. And the IRS has been very, very responsive and very, very understanding. They have been wonderfully supportive to these employees since the attack.

So, like I said, in looking forward I will tell you when the Austin attack happened, even though it was an airplane, IRS employees from around the country felt very, very vulnerable because what they realized was it could have been their building. If the anger was at the IRS, it could have been any IRS building. And it reminded them of things that maybe are more within the control, whether it is about the need for armed guards, whether it is about lighting that isn't working in parking lots, whether it is about cipher locks not working or fire alarms not properly working in the building, things that you identify and you pursue and then something else happens and you kind of lose sight of it. So events like this bring all that back into focus.

But really I have talked to many of these employees and to our local chapter president there, and they have not identified anything that went wrong that day. I mean, it really was a miracle. It was one life too many, but it was a miracle that there were not more.

Mr. CHAFFETZ. And point well taken. I guess we should always continue to probe and understand and look at all the different scenarios, so I would obviously concur with that thought and hope that we continue to expand that.

I guess, Mr. Chairman, one of the points I guess I would take away from that is we should also highlight everything that went right. You can never plan for everything. There is no end to the creativity of these nuts who want to create terror, but at the same time there are a lot of things that went well, and I think we should also highlight and explore and note those, as well.

And perhaps, Mr. Adler or Mr. Wright, you can help me understand where your perception of the FPS, but also the difference between the contractors, if you will, as opposed to those. And help me understand the difference in where you see the fundamental flaws. Either one.

Mr. ADLER. And you are referring, just to clarify, to the FPS inspector versus the contract uniform?

Mr. CHAFFETZ. Yes. The specific concerns about contracting that out. I have real concerns about doing that.

Mr. ADLER. Just from my perspective—and I am going to defer to Mr. Wright—but just, again, by way of background and training, the inspectors go through a different process. The contracting system obviously involves a private company which doesn't place the same emphasis on what it would take to become an inspector, whether it is going through the Federal Law Enforcement Training Center or certain agency-specific training modules. So certainly we place more reliance, if you will, on the inspector, the Federal uniform component within FPS.

Mr. CHAFFETZ. Mr. Wright.

Mr. WRIGHT. The Federal Protective Service inspectors and police officers go through the Federal Law Enforcement Training Center. Nowadays we are up to 24 or 26 weeks of training. The contract security guards are private guards. They have commitments to their companies.

The other thing that needs to be stated in regards to these private guards is they get their authority basically State to State or more likely city to city. There is no Federal authority for a private guard. So in Kansas City, MO, where I come from, the Kansas City Police Department and the St. Louis Police Department have pretty good private watchmen commissions, and they do give the authority to arrest.

Fifty miles up the road in St. Joseph, MO, the first requirement to get a commission there in St. Joseph is that they have a commission in Kansas City. Then 60 miles to the east in Chillicothe, MO, the way you get a commission license is to show your St. Joseph license.

So this goes city to city, building to building, region to region. There just is no common sense there, and that is why one of our recommendations is let's get Federal security guards or Federal police officers, much like you have here at Capitol Police, give these individuals the authority, give them the training, and let them do their job.

That being said, this is not to denigrate any of our contract guards. We have a lot of great veterans coming back and they are being picked up by these private companies, and no denigration at all to those troops, either.

Mr. CHAFFETZ. All right.

Thank you, Mr. Chairman.

Mr. LYNCH. Thank you.

The Chair now recognizes Ms. Eleanor Holmes Norton for 5 minutes.

Ms. NORTON. Thank you, Mr. Chairman.

My condolences, particularly to you, Ms. Kelley, and my thanks to you and to Mr. Adler and Mr. Wright for your service to the United States.

Mr. Wright, I find your charts amazing.

Mr. WRIGHT. Yes.

Ms. NORTON. The charts at the rear of your testimony that rather much point up, I think, the difficulties that we are having with security for Federal employees.

You point to what you call the exponential growth of security and law enforcement staff in virtually every agency except the Federal Protective Service, including a Government-wide growth for the last seven or so years of 56.5 percent, whereas FPS, alone, shows negative growth of 18.4 percent.

Mr. WRIGHT. Correct.

Ms. NORTON. Now, you cite some of these agencies. Doesn't this show that with this huge growth, that first these agencies know they are living post-9/11, so if they can't get it from FPS aren't we in effect forcing outsourcing to whatever contract guards they choose, without any relationship to any central security authority of the U.S. Government?

Mr. WRIGHT. Yes. Just this year, alone, I have heard of agencies coming forward and proposing to hire their own 083 police officers, and actually Social Security is probably the best security-minded agency out there that are our clients, but they have looked into hiring their own 083 police force.

Ms. NORTON. So what we have here, Mr. Chairman, I think, is agencies deciding that, since FPS has been shrinking, since the Federal Government has not been requiring Government-wide security, since we have outsourcing authority, let's set up multiple police forces replicating what the FPS is supposed to do Government-wide, without any central connection to minimum standards for these almost always contract guards and not people who are, as one of you has testified, police officers who go to be trained at the same place where our best police officers in the Federal Government go.

So what we are talking about, I want to just get in the record, multiple police forces popping up, agency by agency, at the agency's discretion, just leaving the whole idea of a Government-wide Federal police force out there to flounder. Is that not the case?

Mr. WRIGHT. Much of that, Ms. Norton, is the way that FPS is funded. We are funded through a security fee of charges per square foot. At this point it is up to $0.66 a square foot. What happens is these agencies see all this money flowing to FPS.

Ms. NORTON. So how do they pay for the outsourced police forces that they set up without any expertise of their own?

Mr. WRIGHT. I don't know.

Ms. NORTON. See, here you have FPS saying you have to have it per square foot, and they say, OK, since nobody is compelling me to use them, who cares about those standards? Let's just hire our own independent police force and make our own standards.

How anybody can tell me that is going to protect the IRS or any other agency, I don't know, but I think it important to note that we are not here talking about what FPS does or shouldn't do; we are talking about the existence of auxiliary police forces, or I

should say alternative police forces in agencies where at will they can decide who they are, what their standards are, with virtually no Federal oversight through the FPS or, for that matter, through the Department of Homeland Security.

What's the relationship, Mr. Adler or Mr. Wright, of the FPS to the local police forces of a particular city or county?

Mr. ADLER. It varies. I think Director Schenkel hit on it. But in my experience what I have seen, there can be a commonality, there can be a camaraderie, but ultimately most local law enforcement, first of all, they are not allowed to carry within a Federal facility. Most of them aren't familiar with the layout. So if you rang the alarm and they came, they might find the front door but they may not be familiar with the layout.

I think the role of local law enforcement, to put it in proper perspective, is really to arrive on the scene quickly to provide perimeter security, crowd control, but really it is incumbent upon the police officers, the law enforcement components within the building working for the agencies to respond and prevent the situation from going from bad to worse.

Ms. NORTON. And I think that is important for the record, Mr. Chairman, since Mr. Schenkel said they depend on local police forces. The notion that busy police forces should do anything but what they would do anyway if there was something on the outside of the business is very disconcerting to hear.

Mr. Chairman, if I could just conclude by noting that in Mr. Wright's testimony—and ask him if he knows what these cities are—he says that at a minimum—it is under FPS structural problems—at a minimum, around-the-clock protection by Federal law enforcement officers should be provided in the 18 to 22 cities with the greatest concentration of employees—meaning Federal employees—and facilities.

I think you say that 24-hour service is only provided in two cities. What are those cities?

Mr. WRIGHT. Can I approach that off the record? I am not sure it is appropriate to say in a public setting.

Ms. NORTON. Yes. Could you make sure that the chairman understands that?

Mr. WRIGHT. Yes. I think you will be very surprised as to who doesn't have it.

Ms. NORTON. Yes. Make sure the chairman gets that in camera so we can understand that. I just think that we know what those—almost anybody could guess what those 18 cities, 18 of 22 cities with the greatest concentration are, and everybody would know that those are the cities that we regard as most targeted, and what your testimony here today has informed us is that we have to get on the stick.

What happened to IRS with extraordinary sadness from all of us was a kamikaze event of the kind that perhaps no police force of any kind could have deterred, but it certainly ought to be a shot across our so-called bow to remember that this is not the kind of attacks we should be expecting, especially in IRS offices.

I work very closely with the IRS here. I have found IRS employees to be among the most collegial, the most customer oriented employees in the U.S. Government. But if you are out here in this re-

cession paying taxes, lost your job, house gone, and you can't find anybody else to be mad at, there is always your local IRS employee, and we have a duty to protect these employees every day of the week that they are on duty.

Thank you, Mr. Chairman.

Mr. LYNCH. Thank you.

The Chair now recognizes the gentleman from Virginia, Mr. Connolly, for 5 minutes.

Mr. CONNOLLY. Thank you, Mr. Chairman.

Ms. Kelley, welcome. I am sorry I was stuck up here the other day, and I thank you for your kind introduction in my absence. In your prepared statement you made reference to the fact that you were shocked at some statements by certain public officials after the tragedy in Austin. Would you elaborate?

Ms. KELLEY. There was a Member of the House of Representatives who—I don't have the quotes in front of me, so I would not want to misquote. I am sure most have seen them in the press, and I would be glad to provide them. And when I issued statements, and also to a Member of the Senate, and when I issued statements expressing shock and disappointment and looking for an apology, they were not forthcoming. Those apologies have never been forthcoming.

I think that it is outrageous that anyone would make statements like those that have been made, much less someone, you know, anyone in a public position that should be supporting Federal employees who are just trying to do their jobs.

Mr. CONNOLLY. If you want to provide more for the record?

Ms. KELLEY. I will be glad to do that.

Mr. CONNOLLY. It would be welcome. Thank you.

Mr. Adler, could you elaborate a little bit? You spoke fast, and although I am originally from Boston, I have lived in the south so long now I have trouble sometimes following a fast presentation, but you were making a point between the difference between, if I understood your testimony, GSA's first screen versus, say, the Israeli approach to security. Could you just elaborate on that a little bit?

Mr. WRIGHT. Yes. We have been addressing this in the TSA venue, as well. The concept of taking proactive steps in the law enforcement security arena, to not simply sit back and become reactionary, become a duck in a barrel, if you will, and pray the barrel is durable enough to withstand the attack, be proactive, but, of course, it is very convenient for me to come here and say we should be proactive. You need resources to accomplish that. You need human beings in uniforms with training and capability and authority to do it.

Out of respect to Director Schenkel, he is making do with what he has, whether it is setting MOUs with local law enforcement or anyone else. Ideally, we would have enough. You know, we are talking about whether we have police officers or inspectors. I would like all of the above. I would love to have police officers at every law enforcement or Federal Government facility, but that would enable us to take a more proactive approach, to have the proper equipment like cameras and so forth so we can monitor the area, have the plain clothes contingent out there who know and are

trained in behavioral actions and just things, little indicators we can pick up.

I know firsthand FPS does an excellent job of that at 26 Federal Plaza in New York. That is the sort of thing that we do want to have happen but, once again, the starting point is having the resources to engage in that type of proactive investigative security law enforcement activities.

Mr. CONNOLLY. Although, as Mr. Miller of the other panel indicated, all of that, if we did everything you just said, it still would not have prevented the terrorist attack in Austin.

Mr. ADLER. Correct. There are two aspects we are talking about here for this hearing. One is prevention, the other is response. We have to concede. Colleen mentioned the plane coming into the building. We concede that. Then we are defined how we respond. So, taking it from initially, the Israeli approach will minimize the prevention side of things, but, and as we all know, human error will occur. Something will get in, whether it is an active shooter or an explosive device. The question then is: what are we trained and capable of doing in response? That was the other side of what I was trying to present.

Mr. CONNOLLY. All right. Thank you. In your testimony you also said, if I heard you correctly, that the IRS puts both the public and its own employees at risk. What were you referring to?

Mr. ADLER. I was referring to quotations that were sent to me. I received a lot of emails. I requested input. I have 65 agencies we represent. Each one has an agency representative. So when the email goes out, they have input. What that was reflecting was I think it is a lot of frustration among my CID special agent members who are concerned that they want to passionately get involved, they listen to what Colleen describes, and they feel as if they have to make it up at game time.

You can't wing it; you have to plan for it and you have to step up and recognize IRS is always going to be a threatened component by virtue of what they do, so you have to commit resources to training the special agents who are there, who are the first responders, to make sure they are not going to make it up when it happens, to make sure they don't have to rely upon somebody who takes the initiative and heroic ability to help in a fire drill or put someone on their back. They should plan, and that will minimize, or actually it will increase their effectiveness in responding to one of these types of attacks.

Mr. CONNOLLY. And in what little time I have left, Mr. Wright, you talked about the FPS being dysfunctional, citing some studies that would say that. If you have a series of recommendations, I would welcome seeing them. One quick question: do you have a view about the relative merits between, say, a Federal guard, Federal employee, versus contract security?

Mr. WRIGHT. As stated earlier, private guards have basically a mish-mash of authority across the United States. Every city, every State is different. The benefits to having a Federal guard, our more likely recommendation is Federal police officers like you have here at the Capitol, they are FLETC trained and they have that Federal authority to immediately stop and detain threats or take action against individuals that enter the property.

What we see now—and I will be glad to share later on the record—a major city where it has been documented—now, I have always had the anecdotal evidence over the years that private guards are afraid to put their hands on anyone. We have documented cases of individuals running from FPS police officers and guards standing by. And just here in the last couple of days I received some very disturbing information where it has been absolutely documented in our operation shield efforts across the country that these guards are witnessing threats or witnessing our attempts to penetrate. We are witnessing these guards say, I can't do anything. I have to stop. If I see something on that x-ray screen that looks threatening, I am not going to stop that individual, I am going to call FPS or in some cases I am going to call the company first. So that is a problem. Federal officers would have that authority right here, right now, stop that individual, take him down, and do what has to be done. You have a lot of private officers out there that are afraid for their own liability.

Mr. CONNOLLY. Thank you. My time is up. Thank you, Mr. Chairman.

Mr. LYNCH. Thank you, Mr. Connolly.

I want to thank the members of the panel for your willingness to come before the Congress and offer your suggestions and offer your testimony.

I am going to leave the record open for 3 days for those Members who are on other committees and haven't had an opportunity to ask questions, but other than that we appreciate your testimony here today and we bid you good day.

[Whereupon, at 4:21 p.m., the subcommittee was adjourned.]

[The prepared statement of Hon. Elijah E. Cummings and additional information submitted for the hearing record follow:]

Opening Statement
Congressman Elijah E. Cummings
Subcommittee on Federal Workforce, Postal Services and the District of Columbia
Hearing on Federal Employee Workplace Security
Tuesday, March 16, 2010, 2:00 pm, 2154 Rayburn House Office Building

Good Afternoon Mr. Chairman. I thank you for calling this hearing on such an important matter...the safety of federal employees.

In recent hearings the Department of Transportation said that safety was their number one priority. Today, we need to hear same message from the Department of Homeland Security.

- January 4, 2010. There was an attack by a lone gunman in a U.S. Courthouse in Las Vegas, Nevada;
- February 18, 2010. There was a suicide plane attack on a federal IRS building in Austin, Texas; and most recently on,
- March 4, 2010. There was a shooting outside of the Pentagon – Headquarters of the United States Military...just a stone's throw away from this hearing room.

Given the recent spike in events, it is not a surprise that federal employees are beginning to have concerns about their workplace safety. They deserve to know what is being done at the respective agencies to protect them from those who desire to do them harm. In each of these instances, there was loss of life—including that of the perpetrator.

Even though we have an established Department of Homeland Security, coordination for security and emergency preparedness response for federal buildings still seems highly decentralized and fragmented. For example:

- The Interagency Security Commission is the primary government body responsible for overseeing government wide standards and coordination for all non-Department of Defense building security, but only employees one full time staff person;
- Congress has mandated that the Federal Protective Services (FPS) employee no less than 1200 staff to coordinate with intelligence agencies regarding potential

threats against 9,000 federal facilities. While they have not dropped below this threshold, the FPS has seen a decline in personnel;

- The United States Postal Inspection Service is responsible for the United States Postal Services' (USPS) security and all related programs including policies and training required to protect USPS assets and its employees. They maintain 650 uniformed Postal Police Officers for perimeter security and other protections of over 32,000 post offices and locations in the US.

In spite of our best efforts at advance planning and the implementation of numerous programs, a disconnect still exists that allows serious breaches in security to occur. On the front lines of the war against terrorism, working to keep our nation safe, you will find the hard working heroes of our military, homeland security, law enforcement, and intelligence community. Through their combined efforts, we have prevented numerous terrorist attacks.

Mr. Chairman, we must continue to work with our Departments and Agencies to strengthen our efforts to provide a safe and secure work environment for our federal employees.

Safety is not a product, but a process. We must continue to examine our policies, improve our procedures and develop innovative solutions so that we stay a one step ahead of the threats we face.

Unless these systems work together efficiently and effectively, we will not be able to prevent terrorist - both home grown and abroad - from disrupting and purposely attacking our nation's civil servants. Safety must be our number one issue.

I look forward to the expert testimony today from our witnesses and yield back the remainder of my time.

Statements and Responses:

NTEU President Colleen M. Kelley continues to respond sharply to irresponsible comments about the Feb. 18 attack on the Austin IRS building that killed one IRS employee and injured more than a dozen others. Here are her statements responding to Rep. Steve King, Sen. Scott Brown and Human Events Editor Jed Babbin (he served as a deputy undersecretary of defense in President George H.W. Bush's administration):

Rep. Steve King's remarks:

From ThinkProgress.com on Feb. 23... http://thinkprogress.org/2010/02/22/king-justifies-irs-terrorism/

TP: Do you think this attack, this terrorist attack, was motivated at all by a lot of the anti-tax rhetoric that's popular in America right now?

KING: ***I think if we'd abolished the IRS back when I first advocated it, he wouldn't have a target for his airplane. And I'm still for abolishing the IRS, I've been for it for thirty years and I'm for a national sales tax. [...] It's sad the incident in Texas happened, but by the same token, it's an agency that is unnecessary and when the day comes when that is over and we abolish the IRS, it's going to be a happy day for America.***

TP: So some of his grievances were legitimate?

KING: I don't know if his grievances were legitimate, I've read part of the material. ***I can tell you I've been audited by the IRS and I've had the sense of 'why is the IRS in my kitchen.' Why do they have their thumb in the middle of my back. ... It is intrusive and we can do a better job without them entirely.***

King: "I think if we'd abolished the IRS back when I first advocated it, he wouldn't have a target for his airplane. And I'm still for abolishing the IRS. I've been for it for 30 years and I'm for a national sales tax. [...] It's sad the incident in Texas happened, but by the same token, it's an agency that is unnecessary, and when the day comes when that is over and we abolish the IRS, it's going to be a happy day for America."

And

From TalkingPointsMemo.com on Feb. 22 ...
http://tpmlivewire.talkingpointsmemo.com/2010/02/steve-king-to-conservatives-implode-irs-offices.php

Rep. Steve King (R-IA) told a crowd at CPAC on Saturday that he could "empathize" with the suicide bomber who last week attacked an IRS office in Austin, and encouraged his listeners to "implode" other IRS offices, according to a witness.

King's comments weren't recorded, but a staffer for Media Matters, who heard the comments, provided TPMmuckraker with an account.

President Kelley Replied
I am outraged at comments attributed to Rep. Steve King in which he apparently claimed to empathize with the man who flew a plane into IRS offices last week and took the life of a dedicated federal employee. The media is also reporting that Rep. King offered to host a fundraiser so that people could "implode" their local IRS offices.

This senseless act of violence cost an innocent man--a dedicated public servant and veteran--his life. Vernon Hunter's family is mourning a husband, father and grandfather and IRS employees are mourning a leader, friend and colleague. Rep. King's comments are inappropriate and show an appalling lack of compassion over his death, as well as a lack of respect for the lives of federal employees nationwide.

Rep. King should retract and apologize for his ill-conceived statements concerning the tragic event that took place in Austin and pledge, as a member of the U.S. House of Representatives, to do everything he can to ensure that the safety of federal employees remains one of our government's highest priorities.

Sen. Scott Brown remarks:

From ThinkProgress.com on Feb. 18... http://thinkprogress.org/2010/02/18/scott-brown-terrorism-yawn/

Newly-minted Sen. Scott Brown (R-MA) appeared on Fox's Neil Cavuto and showed none of the outrage and concern about terrorism that he exuded during his Senate election campaign. Asked for his reaction, Brown said he felt for the families, but quickly shrugged off the attack and transitioned to say that "people are frustrated" and "no one likes paying taxes."

President Kelley Replied
Sen. Scott Brown appears not to understand that Andrew Joseph Stack took the life of a long-time, dedicated IRS employee when he drove his plane into the side of a building housing the IRS in Austin. Rather than condemn the action that has devastated a family and horrified IRS employees across the country Sen. Brown chose to use a media interview to say that the frustrations of the pilot are similar to voter frustrations with Washington. Sen. Brown missed an opportunity to denounce these actions and the thinking that might produce similar actions; he missed an opportunity to express sorrow over the death of Vernon Hunter; and he missed an opportunity to support federal employees who are simply doing the jobs that our country has asked them to do.

I believe that Sen. Brown should rethink his reaction to the tragic events that took place in Austin. He did a disservice to IRS employees and all federal employees in downplaying this senseless act of violence. I would hope that Sen. Brown would make clear that he supports the federal workforce and will use his position in the U.S. Senate to do everything he can to make sure that their safety is a top priority for our government.

Jed Babbin, Human Events magazine editor:

From TalkingPointsMemo.com on Feb. 19 ...
http://www.buzzbox.com/top/default/preview/irs_union_chief_slams_cpac-er-s_austin_plane_crash_joke/?id=529086&topic=CPAC%3AER

Referring to the anti-tax activist Grover Norquist during a speech at CPAC, Jed Babbin said:

And let me just say, I'm really happy to see Grover today. He was getting a little testy in the past couple of weeks. And I was just really, really glad that it was not him identified as flying that airplane into the IRS building.

President Kelley Replied
I am shocked and outraged that Jed Babbin, editor of Human Events, would dare to make light of the tragic event that took place in Austin this week by joking about someone flying an airplane into a government building. This is precisely the kind of irresponsible rhetoric that can turn frustration with policies and politics into attacks on public servants and can contribute to misguided rage against federal workers and threaten their safety.

Mr. Babbin owes IRS employees and all federal employees an apology. We need a more responsible level of discourse in our country about the work of government. Such callous, insensitive statements have no place in our country's public dialogue.

○