

**RISK-BASED SECURITY IN FEDERAL
BUILDINGS: TARGETING FUNDS
TO REAL RISKS AND ELIMINATING
UNNECESSARY SECURITY OBSTACLES**

(111-61)

HEARING

BEFORE THE

SUBCOMMITTEE ON

ECONOMIC DEVELOPMENT, PUBLIC BUILDINGS, AND
EMERGENCY MANAGEMENT

OF THE

COMMITTEE ON

TRANSPORTATION AND

INFRASTRUCTURE

HOUSE OF REPRESENTATIVES

ONE HUNDRED ELEVENTH CONGRESS

FIRST SESSION

September 23, 2009

Printed for the use of the
Committee on Transportation and Infrastructure



U.S. GOVERNMENT PRINTING OFFICE

52-493 PDF

WASHINGTON : 2009

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 TRANSPORTATION AND INFRASTRUCTURE

JAMES L. OBERSTAR, Minnesota, *Chairman*

NICK J. RAHALL, II, West Virginia, *Vice Chair*
PETER A. DeFAZIO, Oregon
JERRY F. COSTELLO, Illinois
ELEANOR HOLMES NORTON, District of Columbia
JERROLD NADLER, New York
CORRINE BROWN, Florida
BOB FILNER, California
EDDIE BERNICE JOHNSON, Texas
GENE TAYLOR, Mississippi
ELIJAH E. CUMMINGS, Maryland
LEONARD L. BOSWELL, Iowa
TIM HOLDEN, Pennsylvania
BRIAN BAIRD, Washington
RICK LARSEN, Washington
MICHAEL E. CAPUANO, Massachusetts
TIMOTHY H. BISHOP, New York
MICHAEL H. MICHAUD, Maine
RUSS CARNAHAN, Missouri
GRACE F. NAPOLITANO, California
DANIEL LIPINSKI, Illinois
MAZIE K. HIRONO, Hawaii
JASON ALTMIRE, Pennsylvania
TIMOTHY J. WALZ, Minnesota
HEATH SHULER, North Carolina
MICHAEL A. ARCURI, New York
HARRY E. MITCHELL, Arizona
CHRISTOPHER P. CARNEY, Pennsylvania
JOHN J. HALL, New York
STEVE KAGEN, Wisconsin
STEVE COHEN, Tennessee
LAURA A. RICHARDSON, California
ALBIO SIRES, New Jersey
DONNA F. EDWARDS, Maryland
SOLOMON P. ORTIZ, Texas
PHIL HARE, Illinois
JOHN A. BOCCIERI, Ohio
MARK H. SCHAUER, Michigan
BETSY MARKEY, Colorado
PARKER GRIFFITH, Alabama
MICHAEL E. McMAHON, New York
THOMAS S. P. PERRIELLO, Virginia
DINA TITUS, Nevada
HARRY TEAGUE, New Mexico
VACANCY

JOHN L. MICA, Florida
DON YOUNG, Alaska
THOMAS E. PETRI, Wisconsin
HOWARD COBLE, North Carolina
JOHN J. DUNCAN, Jr., Tennessee
VERNON J. EHLERS, Michigan
FRANK A. LoBIONDO, New Jersey
JERRY MORAN, Kansas
GARY G. MILLER, California
HENRY E. BROWN, Jr., South Carolina
TIMOTHY V. JOHNSON, Illinois
TODD RUSSELL PLATTS, Pennsylvania
SAM GRAVES, Missouri
BILL SHUSTER, Pennsylvania
JOHN BOOZMAN, Arkansas
SHELLEY MOORE CAPITO, West Virginia
JIM GERLACH, Pennsylvania
MARIO DIAZ-BALART, Florida
CHARLES W. DENT, Pennsylvania
CONNIE MACK, Florida
LYNN A WESTMORELAND, Georgia
JEAN SCHMIDT, Ohio
CANDICE S. MILLER, Michigan
MARY FALLIN, Oklahoma
VERN BUCHANAN, Florida
ROBERT E. LATTA, Ohio
BRETT GUTHRIE, Kentucky
ANH "JOSEPH" CAO, Louisiana
AARON SCHOCK, Illinois
PETE OLSON, Texas

SUBCOMMITTEE ON ECONOMIC DEVELOPMENT, PUBLIC BUILDINGS, AND EMERGENCY
MANAGEMENT

ELEANOR HOLMES NORTON, District of Columbia, *Chair*

BETSY MARKEY, Colorado	MARIO DIAZ-BALART, Florida
MICHAEL H. MICHAUD, Maine	TIMOTHY V. JOHNSON, Illinois
HEATH SHULER, North Carolina	SAM GRAVES, Missouri
PARKER GRIFFITH, Alabama	SHELLEY MOORE CAPITO, West Virginia
RUSS CARNAHAN, Missouri	MARY FALLIN, Oklahoma
TIMOTHY J. WALZ, Minnesota	BRETT GUTHRIE, Kentucky
MICHAEL A. ARCURI, New York	ANH "JOSEPH" CAO, Louisiana
CHRISTOPHER P. CARNEY, Pennsylvania,	PETE OLSON, Texas

Vice Chair

DONNA F. EDWARDS, Maryland
THOMAS S. P. PERRIELLO, Virginia
JAMES L. OBERSTAR, Minnesota
(Ex Officio)

CONTENTS

	Page
Summary of Subject Matter	vi

TESTIMONY

Dowd, William G., Director, Physical Planning Division, National Capital Planning Commission	17
Drew, John E., President, Drew Company, Inc.	5
Goldstein, Mark, Director, Physical Infrastructure, Government Accountability Office	17
McCann, Erin, Resident of the District of Columbia	5
Moses, Patrick, Regional Director, National Capital Region, Federal Protective Service	17
Peck, Hon. Robert, Commissioner, Public Buildings Service, General Services Administration	17
Porcari, John, Deputy Secretary, U.S. Department of Transportation	17
Schenkel, Gary, Director, Federal Protective Service, U.S. Immigration and Customs Enforcement	17

PREPARED STATEMENTS SUBMITTED BY MEMBERS OF CONGRESS

Carnahan, Hon. Russ, of Missouri	48
Norton, Hon. Eleanor Holmes Norton, of the District of Columbia	49
Oberstar, Hon. James, L., of Minnesota	52

PREPARED STATEMENTS SUBMITTED BY WITNESSES

Dowd, William G.	54
Drew, John E.	59
Goldstein, Mark	67
McCann, Erin	84
Peck, Hon. Robert	97
Porcari, John	104
Schenkel, Gary	110

SUBMISSIONS FOR THE RECORD

Dowd, William G., Director, Physical Planning Division, National Capital Planning Commission, responses to questions from the Subcommittee	57
Peck, Hon. Robert, Commissioner, Public Buildings Service, General Services Administration, responses to questions from the Subcommittee	100
Porcari, John, Deputy Secretary, U.S. Department of Transportation, responses to questions from the Subcommittee	107
Schenkel, Gary, Director, Federal Protective Service, U.S. Immigration and Customs Enforcement, responses to questions from the Subcommittee	122



U.S. House of Representatives
Committee on Transportation and Infrastructure
Washington, DC 20515

James L. Oberstar
Chairman

John L. Mica
Ranking Republican Member

David Heymsfeld, Chief of Staff
Ward W. McCarragher, Chief Counsel

James W. Coon II, Republican Chief of Staff

September 21, 2009

SUMMARY OF SUBJECT MATTER

TO: Members of the Transportation and Infrastructure Committee

FROM: Subcommittee on Economic Development, Public Buildings, and Emergency Management Staff

SUBJECT: Hearing on "Risk-based Security in Federal Buildings: Targeting Funds to Real Risks and Eliminating Unnecessary Security Obstacles"

PURPOSE OF THE HEARING

The Subcommittee on Economic Development, Public Buildings, and Emergency Management will meet on Wednesday, September 23, 2009, at 2:00 p.m., in room 2167 of the Rayburn House Office Building to examine existing security level categories in Federal buildings and the allocation of security funds. The Committee will also examine obstacles in providing effective and efficient building security.

BACKGROUND

I. SECURITY IN FEDERAL BUILDINGS

Federal Protective Service

The Federal Protective Service (FPS) is a part of the frontline defense for thousands of Federal buildings, which include Federal courthouses, Social Security Administration buildings, agency headquarters, and other buildings. FPS sends about \$1 billion dollars in executing its mission.¹ The FPS delivers integrated security and law enforcement services to all Federal buildings that the General Services Administration (GSA) owns, controls, or leases. FPS security services are

¹ Government Accountability Office (GAO), *Preliminary Results Show Federal Protective Service's Ability to Protect Federal Facilities Is Hampered By Weaknesses in Its Contract Security Guard Program* (2009).

a “fee-for-service” and FPS customers reimburse FPS for these services through direct billing. FPS services include providing a visible uniformed presence in major Federal buildings; responding to criminal incidents and other emergencies; installing and monitoring security devices and systems; investigating criminal incidents; conducting physical security surveys; coordinating a comprehensive program for occupants’ emergency plans; presenting formal crime prevention and security awareness programs; and providing police emergency and special security services during natural disasters, such as earthquakes, hurricanes, and major civil disturbances—as well as during man-made disasters, such as bomb explosions and riots.

FPS’ protection services focus directly on the interior security of the nation, and require close coordination and intelligence sharing with the investigative functions within Department of Homeland Security (DHS). According to GSA, “FPS is a full service agency with a comprehensive HAZMAT [hazardous materials], Weapons of Mass Destruction (WMDs), Canine and emergency response program as well as state-of-the-art communication and dispatch Mega centers.”² The FPS protects all Federal agencies housed in nearly 9,000 Federally-owned and leased facilities throughout the United States, its territories, and the world. According to FPS data, on an annual basis, the FPS handles: 10 million law enforcement calls for service, including 3.8 million radio calls, 2.4 million telephone calls, and 3.8 million alarm responses; more than 1,000 criminal investigations for crimes against government facilities and employees; arresting more than 4,000 people for committing crimes on Federal property; and guarding more than 500 facilities 24 hours per day, seven days a week.

In the wake of the 1995 Alfred P. Murrah Federal Building Oklahoma City bombing, the Department of Justice (DOJ) assessed the vulnerability of Federal office buildings in the United States, particularly to acts of terrorism and other forms of violence. The United States Marshals Service coordinated the study with GSA, the Federal Bureau Investigation, the Department of Defense, the Secret Service, the Department of State, the Social Security Administration, and the Administrative Office of the U.S. Courts participating.³

The DOJ report made several recommendations to bring each Federal facility up to minimum standards recommended for its security level. Part of the recommendations centered on upgrading the FPS. The report noted that the FPS has the experience and historical character to provide security services for much of the Federal workforce. But, the report also noted that FPS has limited resources to determine building security requirements to address terrorist threats and does not have the resources to respond to these requirements even if the requirements are properly articulated. Furthermore, the report stated that placement of the FPS within the organizational structure of GSA may have limited the ability of the FPS to obtain the resources to assure appropriate security in large, multi-tenant facilities, even when the security needs have been well defined. FPS, according to the report, needs to re-establish its role and take the lead in emphasizing the need for security. The recommendations re-emphasized GSA’s primary responsibility for implementing Federal building security.

The Homeland Security Act of 2002 (P.L. 107-296) transferred FPS from GSA to DHS. FPS is now a division within the Immigration and Customs Enforcement (ICE) agency, which is within the DHS. However, the President’s Fiscal Year (FY) 2010 Budget Request transfers FPS

² GSA, *Fact Sheet of the Security Overview for the Facilities management and Services* (2009).

³ DOJ, *Vulnerability Assessment of Federal Facilities* (1995).

from ICE to the National Protection and Programs Directorate (NPPD) of the Department of Homeland Security (DHS). Chairman Oberstar and Subcommittee Chair Norton have long supported transferring FPS out of ICE. In 2005, they wrote Homeland Security Secretary Chertoff in support of the transfer. The Senate Homeland Security Appropriations Subcommittee supports this transfer in the FY 2010 Homeland Security Appropriations.

Government Accountability Office Review of Security in Federal Buildings

On February 13, 2007, Chairman James L. Oberstar and Subcommittee Chair Eleanor Holmes Norton wrote to GAO to express concern about the Bush Administration's proposal to reduce the number of FPS officers and their presence nationally in Federal buildings. The GAO was asked to examine whether these proposals will adversely affect the Federal Government's efforts to protect the thousands of Federal workers in Federal buildings and the public who use Federal public buildings on a daily basis.

The Committee also asked the GAO to examine the placement of the FPS in DHS and how that placement is affecting the agency's funding, whether the diminished funding has played a role in the reduction in force, and whether a reduction in force poses a significant risk to the Federal workforce and Federal assets.

Pursuant to these concerns, on November 2, 2007, the Chairman and Subcommittee Chair wrote to House and Senate Appropriations Committee Chairman and Ranking Members expressing their support for an amendment to the Homeland Security appropriations bill, which would require that FPS have no less than 1200 Commanders, Police Officers, Inspectors, and Special Agents available to protect Federal buildings.

On July 8, 2009, the GAO released its preliminary report that highlighted some of the ongoing security vulnerabilities in Federal buildings.⁴ The report cited efforts by GAO investigators to penetrate 10 high security buildings with liquid bomb making equipment and to build actual bombs (with inert ingredients) inside the facilities. In each instance, the GAO investigator used entrances manned by security guards using x-ray machines and magnetometers. GAO investigators then entered bathrooms and other areas where they were all able to assemble explosive devices. The Committee staff has received several briefings from GAO as a result of a multi-city investigation on the efficacy of FPS.

The Committee has long been concerned with the funding mechanism for FPS and the lack of a risk-based approach to providing security to Federal facilities. The FPS spends approximately \$1 billion dollars to secure Federal facilities, but the Committee remains alarmed that the Federal Government may not be getting significant value for its investment, given the recent GAO report.

Department of Homeland Security - Interagency Security Committee

The Interagency Security Committee (ISC) was created after the 1995 Alfred P. Murrah Federal Building in Oklahoma City, OK. The ISC is responsible for setting government-wide security policy for Federal facilities. The DHS Assistant Secretary of Infrastructure Protection is the current chair of the ISC. The ISC sets security standards for all civilian facilities that are owned,

⁴ See Footnote 1, *supra*.

leased, or purchased by the Federal Government including standards for physical security, management, and the mitigation of threats.

II. OPEN SOCIETY WITH SECURITY ACT – H.R. 3555

Introduced by Chairwoman Norton on September 10, 2009, H.R. 3555, the “United States Commission on an Open Society with Security Act”, ensures the balance of openness and access, particularly to Federal facilities funded by taxpayers, while maintaining and increasing security against threats posed by global and domestic terrorism. The U.S. Commission on an Open Society with Security Act was conceived in response to the closing of Pennsylvania Avenue NW and when barriers first began to emerge in the District of Columbia after the domestic terrorist attack on the Alfred P. Murrah Federal Building in Oklahoma City, OK, in 1995.

The bill broadly addresses the necessary balance by establishing a presidential commission of experts from a broad spectrum of disciplines to investigate how to maintain democratic traditions of openness and access, while responding adequately to the substantial security threats posed by global terrorism. The Presidential Commission created by the United States Commission on an Open Society with Security Act will focus on the proliferation of increasing varieties of security, from the makeshift checkpoints that were posted on the Capitol grounds, even when there were no alerts, to the use of technology without regard to effects on privacy.

III. SECURITY AND ACCESS TO FEDERAL BUILDINGS

As the Federal inventory of buildings has steadily increased over the last 30 years, the uniformity and implementation of security standards have varied greatly. The Subcommittee will continue to examine these trends and will scrutinize how FPS will continue to provide top flight protection for Federal workers and Federal buildings. Just as importantly, the proliferation of security without any thought to the effect on common freedoms and ordinary access, and without any guidance from the government or elsewhere has led to inconsistent standards throughout the country.

The security in Federal buildings is not uniform and is often set by non-security personnel employed by tenant agencies through a Building Security Committee (BSC) for each individual public building. This approach to security makes it difficult to gauge properly risk in Federal facilities and allocate FPS resources properly. The Subcommittee will examine whether the Transportation Security Administration’s (TSA) uniform airport security model could be applied to Federal buildings to make them safer and offer greater access to American taxpayers.

PRIOR LEGISLATIVE AND OVERSIGHT HISTORY

On February 11, 2005, then-Ranking Member James L. Oberstar and then-Subcommittee Ranking Member Eleanor Holmes Norton wrote to the DHS Inspector General requesting an audit of the use of FPS funds.

On June 14, 2005, Ranking Member Oberstar and Subcommittee Ranking Member Norton wrote to DHS expressing concern about the placement of FPS within ICE, an agency within DHS.

In the 110th, Congress, on February 13, 2007, Chairman Oberstar and Subcommittee Chair Norton requested that the GAO review FPS's budget and personnel, focusing on FPS workforce size, experience, retention rates, and salaries.

On April 18, 2007, the Subcommittee held a hearing on whether the Bush Administration's FY 2008 budget proposal to reduce nationally the number of FPS officers and presence adversely affects the Federal Government's efforts to protect the thousands of Federal workers and visitors to Federal buildings every day across the country.

On June 21, 2007, the Subcommittee held a hearing on weaknesses in FPS's oversight of its contract guard program. As a result of the hearing, Subcommittee Chair Norton introduced H.R. 3068, which banned felons from receiving contracts to provide security for Federal buildings. The Committee on Transportation and Infrastructure reported H.R. 3068 on September 14, 2007. On October 2, 2007, the House passed H.R. 3068 by voice vote. The Senate passed H.R. 3068 with a Senate amendment on September 23, 2008. The House agreed to the Senate amendment on September 27, 2008. The bill became Public Law 110-356.

On November 2, 2007, Chairman Oberstar and Subcommittee Chair Norton wrote to the House Appropriations Committee supporting FPS staffing levels of no less than 1,200 law enforcement personnel.

The Consolidated Appropriations Act, 2008 (P.L. 110-161) requires the Secretary of Homeland Security and the Director of the Office of Management and Budget to certify in writing to the Appropriations Committees that operations of FPS will be fully funded in FY 2008 and to ensure that fee collections are sufficient for FPS to maintain, by July 31, 2008, at least 1,200 staff, including 900 police officers, inspectors, area commanders, and special agents who are directly engaged on a daily basis protecting and enforcing laws at Federal buildings.

On February 8, 2008, the Subcommittee held a hearing on the preliminary findings of the GAO report which had been requested by Chairman Oberstar and Subcommittee Chairwoman Norton on February 13, 2007. The hearing was scheduled because the GAO alerted the Subcommittee to serious preliminary findings concerning the condition of the FPS, and therefore the Subcommittee believed the preliminary report should be placed in the record at a public hearing as soon as possible.

On June 18, 2008, the Subcommittee held a hearing on the final findings of the GAO report. The hearing focused on a comparison of current experience, workforce size, retention rates, and salaries of FPS officers. At the hearing the Subcommittee received testimony from the President of the FPS union, the Director of Physical Infrastructure at GAO, and the Director of FPS. The Committee examined the GAO recommendations on FPS staffing, the inability of FPS to complete its core mission of facility protection, complete building security assessments in a timely and professional manner, and to monitor and oversee the contract guards.

WITNESSES

Mr. John Porcari
Deputy Secretary
U.S. Department of Transportation

Mr. Mark Goldstein
Director, Physical Infrastructure
Government Accountability Office

Mr. Robert Peck
Commissioner, Public Buildings Service
General Services Administration

Mr. William G. Dowd
Director, Physical Planning Division
National Capital Planning Commission

Mr. Gary Schenkel
Director, Federal Protective Service
U.S. Immigration and Customs Enforcement

Mr. Patrick Moses
Regional Director, National Capital Region
Federal Protective Service

Mr. John E. Drew
President
Drew Company, Inc.

Erin McCann
DC Resident

RISK-BASED SECURITY IN FEDERAL BUILDINGS: TARGETING FUNDS TO REAL RISKS AND ELIMINATING UNNECESSARY SECURITY OBSTACLES

Wednesday, September 23, 2009

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON ECONOMIC DEVELOPMENT, PUBLIC
BUILDINGS AND EMERGENCY MANAGEMENT,
COMMITTEE ON TRANSPORTATION AND INFRASTRUCTURE,
Washington, DC.

The Subcommittee met, pursuant to call, at 2:30 p.m., in Room 2167, Rayburn House Office Building, Hon. Eleanor Holmes Norton [Chair of the Subcommittee] presiding.

Ms. NORTON. We are going to reverse the order of the witnesses because, in all fairness, I would like the Federal witnesses to be able to respond to what I think is now the second panel. So you can stay where you are for the moment and our opening statements.

But when we finish with the opening statements, I am going to ask John E. Drew of the Drew Company and Erin McCann, a District resident, if they would take the witness stand. And after their testimony—it is fairly brief—the agencies will have a sense of one of the reasons we have found it necessary to have this hearing.

I want to welcome all of you to today's hearing, especially our distinguished panels.

I called this hearing as Chair of this Subcommittee and a Member of the Transportation and Infrastructure Committee. However, I also sit on the Homeland Security Committee. And I represent the high-target Nation's capital. My committee work puts me in touch with the Nation's security needs at the highest levels. This work and our experience since the Oklahoma City bombing leave no doubt that the complexities of risk-based security in an open society continue to elude us.

Federal building security has little to do with risk-based threats today. The Government Accountability Office was recently able to get bomb-making equipment past security at several Federal buildings in this national capital region, where much of the new security has been focused because of 9/11. At the same time, tax-paying citizens are unable to enter some buildings to use the restrooms or restaurant facilities.

The security in Federal buildings is not uniform where it should be and, sadly, not professional or even appropriately in the hands of the Department of Homeland Security and the Federal Protec-

tive Service. Nonsecurity personnel control much of the security for many agencies.

I introduced H.R. 3555, the "United States Commission on an Open Society With Security Act," on the eighth anniversary of 9/11 this month, as an increasing variety of security measures have proliferated throughout the country without any expert or uniform guidance on evaluating risks to security and without much thought about the effect on common freedoms and citizen access.

Federal facilities, where millions of Federal employees work and citizens come for service, have been the chosen target for major terrorist attacks on our country. After the attacks on the Pentagon and the Alfred P. Murrah Oklahoma City Federal Building, terrorists have left no doubt that Federal facilities, as symbols of the United States Government, are their chosen targets.

Consequently, this documented pattern of terrorist assaults on Federal assets and consistent threats since 9/11 with arrests made even this very week have required continuing high levels of vigilance to protect both Federal employees and the visitors who use Federal facilities.

When the Department of Homeland Security was formed in 2002, the Federal Protective Service, or FPS, charged with protecting Federal sites, was transferred from the General Services Administration to the newly created Department and placed within the Immigration and Customs Enforcement, or ICE. Although the Committee supported the transfer, we insisted that FPS officers and guards be used exclusively by the FPS to continue the necessary protection of Federal sites and those who work and use them.

However, starting in February 2005, the Chairman and I have had to send a series of letters to DHS and this Subcommittee has held hearings questioning the placement of FPS within ICE, inappropriate use of funds, and a major shift from protection to inspection. These concerns have strong bipartisan support, with both Chairman Oberstar and Ranking Member Mica expressing their own views about the gravity of the FPS situation.

Now comes the GAO report to confirm that the FPS, the Nation's first Federal police force, established in 1790, and its contract guard force have been rocked by inadequate funding, staffing, and training that casts doubt on its ability to carry out its core mission: to protect facilities, to complete building security assessments in a timely and professional manner, and to monitor and oversee contractors.

GAO reports, ominously, that pro-active patrols have been eliminated at many GSA facilities in spite of the fact that—and here I am quoting GAO—"multiple governmental entities acknowledge the importance of proactive patrol in detecting and preventing criminal incidents and terrorist-related activities," end quote.

Given the radical changes at FPS at odds with its statutory mandate, who can be surprised that today the GAO will testify concerning how GAO testers were able to get bomb-making equipment past security at several Federal agencies?

At the same time, taxpayers are unable to enter some Federal buildings without escorts or other obstacles to the access to which they are entitled. Surely, we are smart enough to keep terrorists

out without making it virtually impossible for U.S. Tax-paying citizens to get into Federal buildings.

Risk-based security will be impossible as long as the requirements are set by a hodgepodge group who can choose their own security requirements without regard to evaluated risks and the big-picture concerns of each and every region. What passes for security today lacks the needed consistency, rationality, and accountability outside the particular agency. Non-security personnel are setting the agenda and calling the shots, building by building.

We can do better, but only if we recognize and then come to grips with the complexities associated with maintaining a society of free and open access in a world characterized by unprecedented terrorism.

Following the terrorist attack on our country, the first on the continental shores, all expected additional and increased security adequate to protect citizens against this frightening threat. However, the American people also expect government, their government, to undertake this awesome new responsibility without depriving them of their personal liberty.

The place to begin is with a high-level presidential commission of experts from a broad spectrum of relevant disciplines, not military and security experts alone, who can help chart the new course that will be required to protect our people and our precious democratic institutions and traditions at the same time—something we have never had to do before and something we do not yet know how to do.

When we have faced unprecedented and perplexing issues in the past, we have had the good sense to investigate them deeply in order to resolve them. Examples include the National Commission on Terrorist Attacks Upon the United States, also known as the 9/11 Commission, and the Kerner Commission that investigated the uprising that swept American cities in the 1960s and 1970s.

The important difference in my bill is that the commission would seek to act before a crisis-level erosion of basic freedoms takes hold and becomes entrenched. Because global terrorism is likely to be long-lasting, we cannot afford to allow the proliferation of security that does not require and is not subject to expert oversight or analysis of technological advances and other alternatives that can do the security job as well and without the severe repercussions on freedom and on commerce.

Following today's hearing, I intend to move H.R. 3555 to help us find the necessary balance by establishing a presidential commission of experts from a broad spectrum of disciplines to investigate the threshold question of how to maintain democratic traditions of openness and access while responding adequately to continuing substantial security threats posed by global terrorism.

The need for a high-level commission is imperative to look at issues from makeshift security and make-work security, such as checkpoints that are posed in the streets even when there are no alerts to the use of on-the-shelf technology without regard to effects on privacy and openness.

We are open to all suggestions and recommendations concerning what we also do not yet know and do not yet fully understand, and that, of course, is the still-developing work of keeping us safe and

open. We have confidence that our people and those in Federal agencies can do both, keep us open and keep us safe. We have tackled and mastered strong contrasts before.

We will listen carefully to how the agency officials plan to balance keeping citizens safe in an open society. We welcome all the witnesses. Each of you is essential to this hearing, and we particularly appreciate your time and effort in preparing testimony on what we understand to be a very difficult and precedent-setting subject.

I am pleased to ask our Ranking Member, Mr. Diaz-Balart, if he has any opening remarks at this time.

Mr. DIAZ-BALART. Thank you very much, Madam Chairman. Let me thank you for the opportunity, let me thank you for holding this hearing today on the security in the Federal buildings.

If anybody had any doubt, the Oklahoma City bombings and the 9/11 terrorist attacks demonstrated that the Federal buildings clearly are huge targets for anybody who is out there trying to harm us, the United States, and our interests. And the recent arrests in that terror probe I think should also serve to remind us that that danger is still very, very real.

In the wake of the 9/11 attacks, Congress created the Department of Homeland Security, as the Chairwoman has just stated, and transferred the Federal Protective Services from GSA to Homeland Security. Now, the intention was to improve security in our Nation's Federal buildings and facilities. However, despite the importance of security, the GAO has found that serious, serious problems continue to persist. In recent years, the GAO has conducted a number of investigations and reviews of the security in our Federal buildings. Unfortunately, these investigations revealed very significant vulnerabilities.

As highlighted last year before this Subcommittee, the GAO found significant issues with respect to the management and oversight, for example, of contract guard programs. The GAO also found that FPS does not use risk management approaches to link threats and vulnerabilities to resource requirements, raising, obviously, questions as to whether resources are used as efficiently and as effectively as possible.

The potential results of these vulnerabilities, well, is obviously apparent. During a recent review—and the honorable Chairwoman just mentioned this—during a recent review of building security, GAO investigators carrying bomb-making components successfully passed through security checkpoints at 10 Federal buildings—facilities. I am not quite sure if they were buildings, but 10 facilities, Federal facilities.

Now, obviously, resolving these issues is critical to protecting the people that work in those facilities, those that visit the facilities, the tourists, whatever. And that is obviously essential. Ensuring security policies are consistent with and not only consistent but also effective will obviously help balance security with appropriate public access, which is something that we all want to have.

So I look forward to hearing from the witnesses today. I want to thank you. I echo the words from our distinguished Chairwoman about thanking you for being here. I look forward to hearing from you, and these are very important issues.

So I thank you, Madam Chairman, for the hearing.

Ms. NORTON. Well, I appreciate your remarks, Mr. Diaz-Balart.

Of course, the Nation's capital is the easiest site to see. The FPS went far beyond the Nation's capital, however—sorry, the GAO went far beyond the Nation's capital to do its tests. And I see we have the Member from Louisiana, Mr. Cao. If you have any opening remarks, we would be pleased to receive them.

Mr. CAO. I don't have an opening remark, Madam Chair. Thank you.

Ms. NORTON. Thank you very much, Mr. Cao.

Now we will ask our first two witnesses: John E. Drew, president of Drew Company, Inc., and Erin McCann, a resident here in the District of Columbia.

Mr. Drew?

TESTIMONY OF JOHN E. DREW, PRESIDENT, DREW COMPANY, INC.; ERIN MCCANN, RESIDENT OF THE DISTRICT OF COLUMBIA

Mr. DREW. Good afternoon, Madam Chairman and Members of the Committee. My name is John Drew. I am the chairman of Trade Center Management Associates, known as TCMA. We appreciate the opportunity to appear here today, and thank you very much for having us.

I have some prepared remarks, and I will just read from them, if that is all right with you.

Ms. NORTON. Please do.

Mr. DREW. TCMA has had the privilege of being the operator of the public portion of the Ronald Reagan Building in the International Trade Center since the building opened in 1998. We are proud to work with GSA, who is the owner of the building. And, as some of you know, after the Pentagon, we are the largest Federal building, 3.1 million square feet, in Washington, D.C., and the largest in the country.

No one knows better than you, Madam Chairman, that when the Reagan Building was created, it was created with the unique congressional mandate that it was to function as a mixed-use building. One of the main functions included in that mandate is a trade promotion program that we organized to create and enhance opportunities for American trade and commerce.

It is TCMA's responsibility to support GSA in the implementation of this mandate. Specifically, our responsibility is limited to the International Trade Center portion of the building, which consists of public spaces, both inside and outside of the Ronald Reagan Building. It is often referred to as a building within a building. Our team operates the International Trade Center with a diverse workforce and passionate workforce of over 550 full- and part-time staff members.

We are proud to say that the Reagan Building is now Washington's busiest conference and special event location. We produce and provide a wide range of services to over 1,000 meetings and events each year, and we welcome over 1 million visitors to our facilities.

Our meetings and events are diverse and range from the recent U.S.-China economic recovery dialogue that President Obama and Secretary of State Clinton and Treasury Secretary Geithner orga-

nized this July to something that is taking place this weekend, which is a wedding that is taking place this weekend which has been organized by US magazine and the Wedding Channel. So it is a wide variety of activities that are taking place within the building.

In addition, we operate D.C.'s largest parking garage within the building, and that accommodates nearly 2,000 vehicles. This includes hundreds of cars each day that are visiting the Reagan Building for conferences or attending meetings at Federal agencies or driven by people who are touring the city.

We also produce a number of activation projects that help the building fulfill its mission of connecting the central business district with the National Mall. In particular, we host Live on Woodrow Wilson Plaza, which is a free summertime concert series, enjoyed this year by over 75,000 people.

It is worth mentioning that, in order to fulfill the mission of the building and to foster trade, we have a staff devoted to organizing and promoting upwards of 150 trade-related events that take place within the building.

We have a diverse tenant mix within the building. Our public food court has 20 vendors. It serves as a cafeteria for our Federal workforce in the building. It also hosts hundreds of thousands of visitors each year. Many of these visitors are school children who are on organized tours of Washington.

The building is also home to EPA, U.S. Customs and Border Protection, and USAID. In addition, we have private tenants. Tenants are located throughout the building and in the office towers. And they represent private-sector global organizations; the University of Maryland has its business school located in D.C. in the building. International affairs offices of multinational companies are within the building, with foreign trade businesses within the building. We have not-for-profit organizations within the space and, also, international trade consultants occupying the space.

Now that you know more about the facility, my testimony this afternoon will focus on the building security and how it is created and sustained. My remarks are limited to the security environment for the public spaces in the building.

The security is provided by the Department of Homeland Security through the Federal Protective Service using Federal police officers and an armed contract guard force. During normal business hours, the Reagan Building has perimeter security stations at seven different street entrances, including an entrance at the Federal Triangle Metro station. These stations all have X-ray and magnetometers, and everyone entering the premises is required to present a picture ID to a uniformed guard. Some entrances are open around the clock.

In addition, all vehicles entering the Reagan Building are screened using technical means for detecting explosive devices. And, in addition, every trunk and cargo space is inspected by guards.

We also get a large number of trucks making daily deliveries to us and to our food court, restaurants, catering kitchens, and to support events at the conference center. Also, many trucks come to service our Federal tenants. One hundred percent of the larger ve-

hicles are now scanned using a drive-through X-ray machine operated off-site a few blocks from the Reagan Building. It is operated by FPS. All of the drivers have to have been precleared, produce proper ID. And then the vehicles are inspected, and then they are sealed, and then they are reinspected when they enter the Reagan Building before they go to our loading docks. In 2008, 20,000 trucks were inspected through the remote screening location.

In addition to these human and technical security barriers, we also have K-9 officers present on site for random checks, and they respond to any issues that may arise.

As I said, this is just the security apparatus for the public space. The Federal office towers have their own separate security stations and procedures.

Turning back to the public space and International Trade Center, security was increased after 9/11, and perimeter security was installed. Up until then, all 61 doors to the public space were open and accessible with no perimeter security. After 9/11, the measures I described above were implemented.

Initially, we feared that this comprehensive perimeter screening would prove to be an impediment to our conference center guests and our tourist visitors. As it has turned out, everyone seems to have understood the heightened risk and now, I think, believe that, actually, perimeter security is a positive aspect for the Reagan Building.

Of course, this generally positive view of security in the building is made possible because of significant resources and coordination committed by GSA, FPS, and ourselves to make it happen. We have developed a terrific working relationship at the building level and a mutual understanding that security comes first but that the business of government in the Ronald Reagan Building has to continue. We all firmly believe that the building must be open to the public.

Through this cooperation, we have held over 10,000 secured events, with literally millions of visitors. We have developed a strong institutional knowledge that allows everyone to work and function together. This working partnership at the Reagan Building between Homeland Security, GSA, and with the support of our organization, literally continues to grow at all times and every day.

We have established protocols for the visits by the President of the United States, working with the Secret Service. We are also ready for weekly visits by foreign dignitaries to both the Federal space and to the International Trade Center. This is coordinated with the Bureau of Diplomatic Security. The Reagan Building also stands ready for busloads of schoolchildren who come daily to the food court and see the Berlin Wall that we have on display within the building.

Every visitor is security screened through an airport-style X-ray machine, and all packages, backpacks, et cetera, are put through a magnetometer. This kind of seamless and layered security would not exist without close coordination, communication, and cooperation. We have regular weekly and monthly meetings that take place between the Federal tenants and the Reagan Building security staff that meet and talk about security issues and follow through on any updated procedures and other issues.

Members of our own staff participate in a weekly security meeting with the building security to describe all upcoming events. We look 21 days out into the future, and we talk about every event that is coming in within those 21 days. Each event is talked about, it is organized, and then we coordinate each event and event orders for additional guards, deliveries, requests for K-9 after-hours screeners, and we coordinate all VIP parking. This is just to name a few of the security-related requests that we get daily that have to be addressed, and this requires constant communication and coordination.

In conclusion, I think it is worthwhile reiterating that all parties involved recognize that the safety of everyone who works or visits the Reagan Building demands and deserves our daily attention. All parties involved seek practical solutions to maintain the level of security, while ensuring the safety of both the tenants and the guests, and pursuing the mission of the Ronald Reagan Building, to keep it open and accessible, are met.

This concludes my remarks, Madam Chairman. Thank you very much.

Ms. NORTON. Thank you, Mr. Drew.

Ms. McCann?

Ms. MCCANN. Chairwoman Norton, Members of the Subcommittee, I would like to thank you for the opportunity to speak to you today. I have a short statement, and then I will be happy to answer your questions.

My name is Erin McCann, and I am an amateur photographer. I am also an active member of a group called D.C. Photo Rights, which exists to document and discuss incidents in which photographers have been harassed by security officers or police.

In April, I became aware of a series of incidents at the Department of Transportation headquarters in southeast D.C., during which security guards had stopped members of the public from taking pictures of the building. A photographer had written into a forum on the Washington Post Web site asking a columnist for help, and word of the incident spread through the D.C. Photography community. Others shared their own similar incidents, and many headed to the building to see for themselves what would happen when they took their cameras out.

What we have documented since then is a series of incidents going back at least until 2007 during which security officers have stopped photographers for doing nothing more sinister than holding a camera on DOT property. I have attached the details of some of these incidents, including my own. It is important to note that this list is not exhaustive. For every incident someone shared, another photographer would chime in with agreement and say, "Yes, that happened to me there, too."

Many of the officers are polite, but they are firm in their belief that photography of the Department of Transportation or any other Federal building is illegal. Others obscure their names, refuse to provide contact information for supervisors, threaten to confiscate cameras, and issue contradictory orders when questioned.

My own experience started on May 20th. I phoned the DOT security office and spoke with a Lieutenant Hulse, who referred my call to a supervisor. When that supervisor failed to call me back by the

end of the day, I decided to go to the building to see for myself what would happen. Soon, I was standing in a lobby waiting for a supervisor, Lieutenant Butler, who, after taking down the details from my driver's license, made the following points:

When told that DOT seems especially zealous among Federal departments in systematically training its guards to harass photographers, Lieutenant Butler said that made him proud. He said DOT is doing it right and everybody else is doing it wrong.

Lieutenant Butler conceded that most of the people taking photographs of his building are harmless. The number he suggested was 90 percent. If I lived in the version of Washington where 10 percent of the people carrying around cameras were terrorists, I would never leave home.

Lieutenant Butler said his employees are trained to intercept all photographers, collect their contact information, and forbid them from taking any more photographs of the building. This rule is an invasive attempt to collect personal data from law-abiding citizens. Thankfully, the security team often fails to collect such data from the people that it stops.

After this conversation, I contacted the American Civil Liberties Union of the national capital area, which sent a letter to the DOT general counsel's office on May 27th asking for an explanation. I have attached that letter to my testimony. It took 3 months for the Department of Transportation to respond. They apologized for my incident, and they said the guard was in error. They made no mention of the pattern of documented harassment, and there was no indication that any guards would be retrained to end their systematic harassment of anybody with a camera.

By way of defending their attitude toward photographers, the DOT response included a 2004 Homeland Security bulletin regarding photography at Federal buildings. It is a flawed document, claiming that, quote, "a widely known reconnaissance activity of criminal and terrorist organizations has been to gather photographic information about prospective targets." In the age of Google Maps and freely available satellite images, the idea that someone intending to harm a building needs first to conduct his own photographic reconnaissance is laughable. It is also an embarrassing waste of everybody's time.

The DOT is not unique in regarding photographers with suspicion. All around this city and the country, courthouses, train stations, and Federal office buildings have been deemed off-limits to people with cameras. They do so under the mistaken belief that taking pictures in public place is illegal or requires a permit or is an indication that the person holding a camera is somehow a threat. In many cases, people have been detained, handcuffed, and arrested for failing to move along when a guard tells them to.

It is my belief that the time and energy spent questioning every camera-toting tourist could, and should, be put to a more constructive use.

Thank you.

Ms. NORTON. Thank you, Ms. McCann.

I would like to question both of you.

Ms. McCann, I can only say to you that, as a person who practiced constitutional law, I have seldom, in the years I have been

in Congress, heard testimony that, if true, would amount to a violation of the Constitution of the United States subject to a temporary restraining order if the Federal Government had been sued.

The notion that Federal officers would restrain American citizens from exercising their right to express themselves in public, including taking of photographs, is, on its face, unconstitutional. I say that without fear of contradiction. And let me tell you, it is seldom that a careful lawyer would say something as openly as that.

I say it also with deep regret that such a practice has gone on and with apologies to you and those whom you know who have had this to occur. We will try to get to the bottom of it.

I don't want to say—particularly since you have been dealing with people who are only following orders, what your testimony illustrates is responsibility at a far higher level than they. They are people who simply have been told, make sure that you help us protect this building. It is the absence of high-level guidance, even to Cabinet officials, that results in people doing whatever occurs to them, they who have no truly expert terrorist security background, whatever occurs to them. Bearing in mind that we are making it up as we go along, 8 years after 9/11, it is time to try to be more professional than that.

Let me go to Mr. Drew first.

Mr. Drew, I listened, indeed you have been invited here, because we are also going to hear from those who control of the other side of the Ronald Reagan building, but we invited you here precisely because perhaps the Ronald Reagan Building provides us with the best example of contracts, only this time we are not dealing building-to-building contracts, as we see throughout the region, where you do not know and where there is absolutely no consistency building to building.

Here we have a real test case within the same facility, a highly secured facility at that, on the one hand with the Federal agencies. And then, on the other hand, I can tell you, because as I entered Congress this was part of the first work I did, was to say to the Ronald Reagan Building, "Pay for yourself. Run it like a private enterprise. Get as many"—I was cheered to hear there would be weddings there—"Get as many different kind of people who can pay the price in." And, by the way, also to insist, as we did, that this had to be a trade facility and not an ordinary office building. So you will get pretty highly placed foreign officials who, were we unable to protect them, would embarrass the United States of America very severely.

So you give the word "mixed use" new meaning. Normally we don't mean mixed secure and highly secure use. And you also give new meaning, the notion "public-private," because you have a private facility as part of a large landmark public facility, at the time the largest since the Pentagon.

Let me, therefore, ask you a set of questions. I was particularly interested to hear you talk about the parking garage. Who may enter that? What kinds of clientele enter that garage?

Mr. DREW. It is open to the public.

Ms. NORTON. So does that mean Federal workers on the one hand and people who are coming for events on the other?

Mr. DREW. Yes.

Ms. NORTON. Now, if people are coming for an event, there is a premium put on making sure they get there in time for the event to take place. How are you able to accomplish that, if you are, while keeping the building secure for all its purposes and all of its uses may flow through there for parking purposes?

Mr. DREW. Madam Chairperson, the way it is done in our case is that our people who are involved in sales and events make it known to anyone who is attending events or running events at the building that we are in a secure building. And we describe the security and—

Ms. NORTON. So when they are contracting for the building.

Mr. DREW. Exactly. So it really is part of the communication that we have with someone who is going to be using the building. And so they are aware of it before they ever—and their guests, we hope they make their guests aware of it before they ever come to the building.

The protocol that I described, that FPS put together, about checking the vehicles and examining the trunks and looking with mirrors below the vehicles has been established and put in place after 9/11, and it is followed for every vehicle that is coming into the building.

So people know that this will take place. It doesn't mean they have to take extra time, but we also explain, quite frankly, that once you are in the building you are also in a protected environment. And that we turn into as much of a positive as possible.

In our case, I think the secret is a day-to-day and week-to-week working relationship, where there is constant communication and these weekly meetings that take place.

Ms. NORTON. And who is in on those weekly meetings?

Mr. DREW. The FPS is in on those meetings. The contractor, CIS is in on those meetings, and our staff is in on those meetings, as well as the GSA.

And we, in fact, we have learned by literally working together since 9/11 how to, in fact, brief one another, I think, very thoroughly. We also, in those weekly meetings, look at the past week's experience, of the past 10 days' experience, and we talk about events that have taken place. And so, if there are any learnings that we have from what we did last week, we are sharing those learnings. So it makes, I think, for a very collaborative operation.

And to give credit to the team that we have, we, as a staff, pay particular attention to the fact that we are part of the security operation, too. Our people keep their eyes open, keep their ears open, and if there is anything they think is unusual they make it known to the security team.

Vice versa, what we work with the security team on is trying to see, in their policing and security function, how we can introduce some hospitality there, so that people are moved through quickly but the work is done thoroughly, and have people understand, for example, if we have a lot of people coming between 6:00 and 7:00 tonight, that we expect to have so many hundreds of people that might be coming in, the entrances that they will be using, and what they can anticipate—what type of people they are and what they can anticipate.

So there is an awful lot of time—

Ms. NORTON. You mentioned protocols of the Secret Service. That is set protocols, is that right?

Mr. DREW. Those are set protocols.

Ms. NORTON. That means if the President of the United States were to come tonight, you wouldn't have to start all over again—

Mr. DREW. Not at all.

Ms. NORTON. —to figure out how to make sure he could sit in the same building with others.

Mr. DREW. Right.

Ms. NORTON. Question for Ms. McCann before I ask the Ranking Member and before I go forward: Have you been able—you described how others came out, as well. Did they come together with their cameras, or were they testers, also, one at a time?

Ms. MCCANN. Mostly one at a time. The deal with the DOT headquarters building is that it is right next to the Nationals Stadium, and people cut through next to the building on their way to baseball games. So there are certain nights where there are massive numbers of people walking by, many of them carrying cameras.

Ms. NORTON. Were any of them able to, in fact—of course, those games take place in the day and take place in the evening. Were any of them able to photograph the building without interference?

Ms. MCCANN. Yeah, it does happen—

Ms. NORTON. There is no consistency on when you can or not based on the time of day or any of the rest of it?

Ms. MCCANN. In my experience, it depends on what guards are working. And that is kind of the way it works at other Federal buildings. I had a friend who was told in front of the Justice building that he couldn't photograph in front of that building, but that was a one-time incident. He went back the next night, and a different guard was working and didn't stop him. And that is—

Ms. NORTON. And no one told you about a policy or cited to you a policy or cited to you a document or cited to you a law that governed their discretion?

Ms. MCCANN. The guard that I spoke with, Lieutenant Butler, cited Title 18 of the U.S. Code, which I believe is the entire U.S. Criminal Code.

Ms. NORTON. I believe you are right.

Ms. MCCANN. And that was the best that he could give me.

Ms. NORTON. And, again, I stress that he is only doing the best he can. And I also stress that I think the agency heads are only doing the best they can.

There is no central authority that consistently advises agencies or guides them, so that while you see some of this as laughable, it all comes back to the Federal Government, which is why this hearing is being held, not because we think any fool would know what to do. On the contrary. If you don't know what to do, then make it up so that you protect as much as you can.

I want to ask the Ranking Member if he has any questions.

Mr. DIAZ-BALART. No. Thank you, Madam Chairman. I am fine.

Ms. NORTON. Let me go back for this question to Mr. Drew.

Is there an agreed upon—here you have very secure and secure. And let me just say, Mr. Drew, that I am looking at what you are doing because I think what you are doing is instructive for the very large private sector in this city and in the Nation. Equally unin-

formed and without guidance are the far greater number of private facility owners, and they have been out there doing catch-as-catch-can. They can't call upon the government. They have to do whatever they can. They, like you, have a bottom line, which is: We better be open for people, or else we stop commerce in our building and in our jurisdiction.

But one of the reasons that I want a presidential commission or some high-level commission, frankly, is not simply to guide Federal officials but because I don't think there is a lot of difference—and I think you show it—between the private and public sectors.

Most public agencies are pretty low-level targets, quiet as it is kept, for terrorists. And yet many of them, I would say in their hubris, but I think in an overabundance of caution, regard themselves as susceptible tomorrow.

So my question becomes, you have one building; conceivably, you could have something happen in the public or private side, and then it is everybody who is affected. Is there a security plan for the entire building?

Mr. DREW. Yes, there is. And that is with the FPS is responsible for. We are working on our side of that building, but FPS is working with the Federal agencies for the other side of the building, and they bring it together.

I think there is a lot of—I can't speak to specifically what is taking place within the Federal space, because that is not where we go. But the—

Ms. NORTON. Well, and some of that would be secure. And you meet and have discussions. I am now hypothetically envisioning something happening in one part of the building that technically didn't happen at all and perhaps wasn't even known about in the other part of the building. I am trying to see how those who are not affected, those who are directly affected would respond to such an incident.

Mr. DREW. That is a very good question. What we would do in that case is that we would either notify, if it was on our side of the building and we find something was occurring, we notify the command center. The command center would work with FPS, and the entire building would be in fact then engaged.

Ms. NORTON. And the command center is run by whom?

Mr. DREW. The command center in our building is run by the contracting service. But I must point out, one of the, I think, special features of the building is it is immediately next-door to FPS, so they are side by side. So even though they are manning the command center, staffing the command center, it really works as one unit.

Ms. NORTON. You are leasing—sorry. You have a contract?

Mr. DREW. We have a contract with GSA. Under that contract, what we have responsibility for is the public space. But that is the sale—that is basically event sales, leasing the private-sector parts of the building, overseeing the parking garage from an operations—

Ms. NORTON. So you lease the garage yourself?

Mr. DREW. No, we operate it for GSA. So we are below GSA operating it. So the protocols for—

Ms. NORTON. Okay. So within the GSA lease—

Mr. DREW. Yes.

Ms. NORTON. —you have responsibility for the garage.

Mr. DREW. Within the GSA contract that we have, as opposed to a lease, we have responsibilities for the garage.

Now, those responsibilities are in providing service in the garage. So we manage, you know, you when you come to the garage, collect your money, help you park your car, all of those things, get your car back and then leave.

Ms. NORTON. Now, have you been given guidelines, Federal guidelines? How does GSA or DHS evaluate whether or not what you are doing in the private side makes that building safe for the public side?

Mr. DREW. We are not evaluated on safety. We are evaluated on service, by GSA.

Ms. NORTON. So how do we know that the building is secure if you are not evaluated on security? Is anybody in charge of doing that?

Mr. DREW. The FPS is team is in charge of doing that.

Ms. NORTON. So what do they do?

Mr. DREW. Well, they, in fact, have a very rigid program and, I think, a pretty thorough program established, where every vehicle is inspected. And if you are a tenant in the building and you have an ID, you can show your ID and you can proceed into the garage.

If you are a tourist or a visitor coming to the building, you, in fact, show your driver's license, but then your car is inspected, your trunk is opened, cargo space is inspected. In addition, there is a mirror put below your car to see if the car is also safe. And then they have a way of checking the car for explosives, which I can't explain to you, Madam Chairman, but they have a technique set up there where they will wipe the car and make sure there is no explosives around that car before they let you proceed into the garage.

Any large truck cannot come into the garage or come into the loading dock unless it has gone through the off-site X-ray system.

Ms. NORTON. That interests me very much. Do you know whether or not there are other buildings, Federal buildings, that use this inspection service for garages?

Mr. DREW. I believe they do. FPS can speak to it, but I believe the other buildings use it, as well.

So a small truck can come in and be inspected on site, but anything that is larger, a cargo truck—and it is because of the quantity that the larger trucks can contain. So those are all taken off site. And they are checked, they are inspected for cargo, they are sealed. They have 20 minutes to come to the building. If they don't get to the building within 20 minutes, they have to go back through the procedure again. The seal is checked at the building to make sure it hasn't been tampered with. The driver's ID has been checked, and the driver has been recorded.

So it is pretty thorough program in place to manage the garage to make sure it is safe.

Ms. NORTON. If someone went out into that large, beautiful courtyard by the Ronald Reagan Building and decided to take pictures, Ms. McCann or anybody else, would anyone stop such a person today from doing that?

Mr. DREW. I don't believe so. I mean, and the reason I can say that with some certainty is that, for example, today—

Ms. NORTON. Do you have guards separate from their guards?

Mr. DREW. No, we don't. All the guards are connected with the building. We don't have our own guards as part of TCMA.

But the guards within the building go out into that courtyard for lunch. We have a concert, a free concert, going on there today. There are many people out there with cameras, and they are taking pictures of the concert as well as, I presume, the building.

Ms. NORTON. Have you had complaints from members of the public about how tough it is to get into the building?

Mr. DREW. Once in a while, yes. But, again, I think we defend—we take those on directly, and, quite honestly, we are not apologists for the security. We really explain why the security is beneficial to them if they are coming into the building and beneficial to us.

Ms. NORTON. Have you ever found yourself with the cars backed up out into Pennsylvania Avenue trying to get in?

Mr. DREW. Once in a while.

But I will give you the opposite of that. We have had some events where there has been a lot of trucks bringing in exhibits, for example, that are going to be displayed within the building. And the FPS has worked with us to keep the X-ray site open after-hours. We pay for that extra expense; it is at our cost. But they have done that on large events. But it is because it is coordinated, we have told them in advance, and we have planned it. We have also used dogs and K-9s on trucks that are coming in after-hours as a way of expediting people coming in and out of the building.

You know, I must say, it is a work in—it is a work every day that is in progress. And I think every day we try better to make it easier. But at the same time—

Ms. NORTON. And you weren't a security expert when you took over this building.

Mr. DREW. I am not.

Ms. NORTON. So you, essentially, worked hand in glove with whom?

Mr. DREW. We worked hand in glove with the team at GSA, in particular, and then with—

Ms. NORTON. So you all figured it out. You worked it out. GSA understood, or FPS, whoever, that you had a mandate to hold events there. And was there a great deal of friction among you on this matter?

Mr. DREW. I must tell you that, first of all, because of the legislation, because of the work that you did and others did, but you in particular did, in creating the Reagan Building, we have a special piece of legislation that is there that was created, a Pennsylvania Avenue development group. And so the purpose of the building has never been questioned because of that legislation. It is meant to be open to the public. It is meant to be, as you said, profitable, paying for itself, et cetera. So, with that guideline, I think people have respected that guideline, and that has made it possibly easier, in our case.

But I do recall that, right after 9/11 and with all of the anxiety, we had some that felt that the building was best if it was sealed off and closed. But because of the legislation and because of the be-

lief in the legislation that the team, in particular GSA, had, they stood by us. And then, once we said, "No, the building has to be kept open to the public," it became a question of how to do it. And then I think the minds all got together and the cooperation began.

And we had some stumbles. I mean, we have worked together and, I think, have helped each other out. And we have learned, as I said, on a daily basis how to do it better. And I don't know if we are doing it to anyone's complete satisfaction, but we try to do it better every day.

Ms. NORTON. And you make an important point. You had a mandate. You follow the mandate. It was a public-private mandate, but it was an unprecedented mandate. Instead of throwing up your hands or using the public mandate to defeat the private mandate, you did what we can only expect Federal agencies to do now.

There is no template for this. We have to create the template and to be open and flexible enough to do it, rather than slam on the brakes and close up the society.

Ms. McCann, you gave testimony before us concerning use of cameras at another monumental site, the Union Station, where we have heard some of the same things you have said about the DOT building.

First I have to ask you whether or not, since you testified in March of 2008 on what appears to be the same things you are now finding at DOT—guards stopping people from taking pictures, no text or guidance to point to, no training—have you seen any measurable change in the policy at Union Station?

Ms. MCCANN. Absolutely, yeah. I walk through there every single day, and I am always looking for people with their cameras. And I walk through every couple of weeks with my own camera and walk upstairs and downstairs just to check, because I am genuinely surprised that it hasn't reared up again. But it is been consistently open regarding photography since we had the hearing last year.

Ms. NORTON. Well, I have to give you and your testimony credit. And, of course, we use that to say to Union Station, one, take down the sign that said, "This is private property"—

Ms. MCCANN. It took them about 2 months to take that sign down, too.

Ms. NORTON. Absolutely. That bothered us. Two months to take down a sign saying that a monumental public possession of the United States of America is private property.

Okay, you all got that done. Let's say whether or not people can take pictures, pictures of what we want them to take pictures of, the extraordinary new rendering of the historic Union Station.

And I think the Union Station knew it also required new training for guards. We had everybody before us, including Amtrak, those who use the station in any way. And we have seen that oversight does produce—and we didn't have to do any new law, we didn't have to do any new regulation—that oversight has been enough to get changes in one monumental site.

Without a lot of oversight on this issue—we have done oversight on Ronald Reagan Building—we see that the agency is using the statute, have figured out how to do it. I say that the Federal agencies have lacked that oversight. And even as I have been very critical, the buck stops right here, right in the Congress, and right

with the agencies who have some oversight, including Department of Homeland Security, including our own transportation agency.

But we caution agencies, again, that people sitting in Congress are not always alert to difficulties until you bring it to our attention. Then the agency is in a much better position than to have people like Ms. McCann bring it to our attention. And then we then have to say to the agency, how come you haven't done something about this?

So we sit here today to use your examples to help us who know least about this and to help the agencies across the United States, and particularly in this high-targeted region, find the balance. And I alert you that, in the region struck by 9/11, I can't afford to err against homeland security. And I think you have showed us that we need not choose to do that.

Ms. NORTON. Thank you very much. We will call the next set of witnesses. Thank you for your patience. We will just proceed right across the board beginning with Deputy Secretary Porcari, of the U.S. Department of Transportation.

TESTIMONY OF JOHN PORCARI, DEPUTY SECRETARY, U.S. DEPARTMENT OF TRANSPORTATION; MARK GOLDSTEIN, DIRECTOR, PHYSICAL INFRASTRUCTURE, GOVERNMENT ACCOUNTABILITY OFFICE; HON. ROBERT PECK, COMMISSIONER, PUBLIC BUILDINGS SERVICE, GENERAL SERVICES ADMINISTRATION; WILLIAM G. DOWD, DIRECTOR, PHYSICAL PLANNING DIVISION, NATIONAL CAPITAL PLANNING COMMISSION; GARY SCHENKEL, DIRECTOR, FEDERAL PROTECTIVE SERVICE, U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT; AND PATRICK MOSES, REGIONAL DIRECTOR, NATIONAL CAPITAL REGION, FEDERAL PROTECTIVE SERVICE

Mr. PORCARI. Thank you. Chairwoman Norton, Ranking Member Diaz-Balart, and Members of the Subcommittee, on behalf of Secretary Ray LaHood, thank you for inviting us here to discuss the security practices and the policies for the Department of Transportation headquarters.

I am pleased to say that the Department of Transportation is enjoying its new headquarters building. It is working out very well, and we are excited to be part of the redevelopment that is occurring in the Capital Riverfront area of Southeast Washington. There was a strong commitment by the Department of Transportation leadership at the time to provide a safe and secure environment for its employees and to comply with post-9/11 recommended security measures in the design and construction of the facility to mitigate risks. The requirements for the DOT headquarters represented the government's security consultants recommended industry practices, and were reviewed and adopted in collaboration with the Federal Protective Service and the General Services Administration. The DOT headquarters security requirements were developed consistent with the prevailing Interagency Security Committee security design criteria, the GSA policy guidance on 50-foot setbacks issued on April 2002, and a detailed risk assessment and analysis that was conducted specifically for the Department that validated that the requirements were appropriate for a cabinet agency with mission essential functions.

Madam Chairman, DOT learned well the lessons of Oklahoma City and was directly affected by the loss of valued employees in that senseless act of violence. Prior to the Oklahoma City bombing in 1995, as you pointed out, there were no governmentwide standards for security at Federal facilities. Today, in this facility that is designed to the best available standards, the Department strives to not only provide a safe and secure environment for its employees but also to be a good neighbor. Our 5,900 employees in the building support local businesses, and I am pleased to say that DOT has been recognized by the Capital Riverfront Business Improvement District for our efforts to be a good neighbor.

We host a farmer's market open to all in the neighborhood every Tuesday, in season.

On Wednesdays at lunchtime we host local musicians while vendors provide food and refreshments, and in the evening movies are shown behind our building for the benefit of neighborhood residents.

Thursdays are open market days where local vendors can offer their wares.

And beyond those daily good neighbor activities, we have also accommodated planned special events like the District of Columbia's Presidential Inaugural event which was held in the building in January.

The security practices and policies for the Department of Transportation headquarters building conform to Federal standards. Because of the new construction opportunity we have been able to integrate post-9/11 security measures that have greatly enhanced the security posture of the DOT headquarters building compared to many existing government facilities, and we are grateful for that. Overall, the security practices and policies for the Department's headquarters building are equivalent to other cabinet agency headquarters here in the District of Columbia.

Thank you for the opportunity to testify, and I will be happy to answer any questions.

Ms. NORTON. Thank you very much, Secretary Porcari.

Next, Mark Goldstein, Director, Physical Infrastructure, Government Accountability Office.

Mr. GOLDSTEIN. Thank you, Madam Chair and Members of Subcommittee. We are pleased to be here today to discuss the Federal Protective Service's efforts to ensure the protection of over one million government employees as well as members of the public who work and visit the Nation's 9,000 Federal facilities.

There has not been a large scale attack on a domestic Federal facility since the terrorist attacks of September 11 and the 1995 bombing of the Murrah Building in Oklahoma City, Oklahoma. Nevertheless, the recent shooting death of a guard at the U.S. Holocaust Memorial Museum, though not a Federal facility, demonstrates the continued vulnerability of public buildings to domestic terrorist attack.

My testimony today discusses issues from completed GAO reports as well as ongoing work we are conducting for the Subcommittee. Overall we have found that FPS faces a number of challenges that hampers its ability to protect government employees and the public in Federal facilities. These challenges include, devel-

oping a risk management framework, developing a human capital plan and better oversight of its contract guard program. A summary of our finding follows.

First, as our July 2008 report showed, FPS' approach to protecting Federal facilities did not use a risk management approach that links threats and vulnerabilities to resource requirements. While FPS has conducted risk-related assessments such as building security assessments, we have reported concerns with the quality and approach that FPS uses to conduct these assessments. For example, FPS' approach is not allowed to compare risk from building to building so the security improvements in buildings can be prioritized.

Further complicating FPS' ability protect Federal facilities is the building security committee structure. In some of the facilities that we visited, security countermeasures were not implemented because building security members could not agree on what countermeasures to implement or were unable to attain funding from their agencies.

Second, as discussed in our recently released July 2009 report, the absence of a strategic human capital plan to guide its current and future work force planning efforts is another significant challenge confronting FPS. The agency has begun taking steps toward developing a work force transition plan to reflect its work force reductions that have been required several years ago. However, in 2008 FPS discontinued this plan because its objective was no longer relevant because of Congressional mandate to increase its work force. FPS experienced difficulties meeting this mandate in part because of challenges to shifting its priorities from downsizing the work force to increasing it to comply with the mandate and delays in the candidate screening process.

Additionally, we found that FPS headquarters does not collect data on its work force's knowledge, skills, and abilities. Consequently, FPS cannot determine what its optimal staffing levels should be or identify gaps in its work force needs or determine how to modify its work force planning strategies to fill these gaps.

Third, as we testified in a July 2009 congressional hearing, FPS does not fully ensure that its contract guards have the training and certifications required to stand post at Federal facilities. While FPS requires that all prospective guards complete 128 hours of training, including 8 hours of x-ray and magnetometer training, it was not providing some of its guards with all the required training in the regions we visited. For example, in one region, FPS had not provided the required 8 hours of x-ray or magnetometer training to its 1,500 guards since 2004. Insufficient x-ray and magnetometer training may have contributed to several incidents at Federal facilities where guards were negligent in carrying out their responsibilities.

In addition, FPS has limited assurance that its contractors and guards are complying with the terms of contract and post orders once they have deployed to a Federal facility. For example, with the components for an improvised explosive device concealed on their persons, our investigators passed undetected through access points controlled by FPS guards at 10 level IV facilities in four major cities where we conducted tests. Of the 10 facilities that we

penetrated, eight were government owned and two were leased, and they included the offices of a U.S. Senator, a U.S. Representative, as well as agencies such as the Department of Homeland Security and the Department of Defense. Once our investigators passed the access control point they assembled the IED from the materials they were able to get past the guards.

We also noted that CERTS, FPS' primary system for monitoring and verifying whether guards have the training and certifications required to stand posts at Federal facilities is also not fully reliable. We reviewed training and certification data for 663 randomly selected guards in six of FPS' 11 regions and found that 62 percent of the guards who were to deploy to a Federal facility had at least one expired firearm qualification, background investigation, domestic violence declaration, or a CPR first Aid training certification. Without a domestic violence declaration in place, guards are not permitted to carry a firearm. FPS requires almost all of its guards to carry such weapons.

Finally, while FPS has taken steps to improve its ability to better protect Federal facilities, it is difficult to assess the impact of these actions because most of them occurred recently and have not been fully implemented. Moreover, there are a number of factors that will make implementing and sustaining these actions difficult.

First, FPS does not have adequate controls to monitor and track whether its regions are completing the new requirements.

Second, FPS has not modified any of its 129 guard contracts to reflect these new requirements.

Third, FPS has not completed any work force analysis to determine if the current staff of 930 law enforcement security officers will be able to effectively complete the additional inspections and provide the x-ray and magnetometer training to 15,000 guards in addition to the current physical and security law enforcement responsibilities. And while we are pleased that the new RAMP system will modernize how FPS manages its mission, we remain concerned about the accuracy and reliability of the information that will be entered into RAMP, including data from CERTS where we have noted problems.

Madam Chairman, this completes my statement. I will answer any questions that you may have later.

Thank you.

Ms. NORTON. Thank you, Mr. Goldstein.

Robert Peck, Commissioner, Public Building Service of the GSA.
Mr. Peck.

Mr. PECK. Thank you. Madam Chairman, Mr. Diaz-Balart and Members of the Subcommittee, my name is Robert Peck, and I am, once again, the Commissioner of the Public Building Service at GSA. I have been here before. Thank you for inviting us to the hearing today. I have a statement for the record. I am going to summarize it and invite you to ask questions.

We have no more important responsibility in GSA than safeguarding the one million Federal tenants in our buildings and the people who come to visit them. It is the most difficult responsibility to undertake because we have the responsibility both of safeguarding them and also of maintaining the freedoms that are the very reasons that our buildings and our government exists.

It is somewhat easier to secure a high security facility somewhere in the middle of nowhere, put a huge fence around it, say nobody can get in and authorize your guards to use deadly force to keep out intruders. We are in the opposite position. We want people to visit. We want people to feel like these are their buildings. It is a very tall order.

Can I just say as an aside to Ms. McCann, as a student in the early 1970s working on a paper on government architecture, I also tried to take a picture of a government facility in downtown Washington and was thrown out by a guard. So it is not just a new phenomenon and it is something that has been going on a long time. I also thought it was totally illogical.

I will just say this is an important enough responsibility to me that one of my first actions coming back into GSA was to attend a national meeting of the Federal Protective Service in Kansas City and to talk to their regional heads and to Mr. Schenkel, their National Director. When I came to GSA the last time it was 8 months after the Oklahoma City bombing, and I spent a lot of time on security. We were in the process of developing security standards and spending a lot of money on countermeasures, and we learned a lot over the 5 years after that I was at GSA.

The events of September 11, 2001, obviously, increase the urgency of security measures in government and other facilities and there have been lots of changes since then, I think mostly for the better. The Interagency Security Committee, on which GSA sits and on which we are the only agency with a primary real estate responsibility, has in fact tightened its standards and attempted to make those standards more based on risk of the kind of agencies in the building, the location of buildings, and the very structure of the building themselves. I think there is still a lot of work to be done.

Obviously since then the Federal Protective Service has moved to Homeland Security, and although we are no longer totally joined at the organizational hip, there is no less important a call on all of us for GSA and Federal Protective Service to work together.

Our job with the Federal Protective Service and our customers, the agencies who occupy our buildings, is to balance the risk, the resources we have available, functioning in the buildings as government agencies, and allowing in the public. How are we doing with all of that? I would say, as I said, better than we have before. I think there is a lot of work remaining to be done.

I will say that you have raised some important issues at the hearing today about whether there is consistency in the way we go about doing that among our agencies. And so let me focus on that just for a brief moment.

It is very important that we have an overall framework in which we assess the vulnerability of our buildings and in which we assess the risks and balance those risks against the resources we have available. It is also important to customize the security in our buildings because some agencies require more vulnerability, some locations require more vulnerability, more or less rather countermeasures against those vulnerabilities. I have some questions about the way we have gone about it and I think they parallel yours.

I believe that in many cases the way in which the building security committees are organized and the authority that building security committees have, now called facility security committees have, to assess their own countermeasures is perhaps misplaced. I question—one of the suggestions I would make is that at a higher level inside our government I believe we need to have the kind of a framework that will allow FPS and GSA to go to the individual security committees and have an overlay in which we say, we understand your concerns, but we have experts who know how to do this kind of work and we are going to balance those kinds of concerns of yours as tenants with the resources and the expertise that we have as security experts.

I will say again I am brand new to the job. This is my sort of first assessment of what is happening in our security business, and I look forward to working with you to figure out a way to make those changes.

Ms. NORTON. Thank you, Mr. Peck.

William Dowd, Director of Physical Planning Division, National Capital Planning Commission. Mr. Dowd, you are next.

Mr. DOWD. Yes, ma'am. Good afternoon, Chairwoman Norton and Members of the Subcommittee. My name is Bill Dowd and I am the Director of the Physical Planning Division at the National Capital Planning Commission, which is the Federal Government's central planning agency for the Nation's capital. It includes representatives from the Department of Interior, the Department of Defense, General Services Administration, the Mayor of the District of Columbia, the Council of the District of Columbia, United States House and Senate Committees with oversight responsibilities in the District, and individuals appointed by the President of the United States and the Mayor of the District of Columbia. I am very pleased to have this opportunity to speak with you today about NCPC's role in trying to balance legitimate needs for physical security with the undesirable impacts to important public spaces in our Nation's capital.

Unlike other cities across the country, as the seat of our Federal Government, Washington, D.C. Has a significant concentration of Federal office buildings, museums and national icons that warrant levels of protection. The most typical and visible form of physical security in the city is vehicle barriers located in our treasured public spaces. These public spaces include sidewalks and building yards, accommodate a vast range of uses, and provide for mobility and enjoyment by the public; however, barriers sometimes detract from sense of openness that is so important to our capital city.

In the National Capital Region, NCPC is responsible for the oversight of all physical development proposals on Federal land and, as such, has developed extensive firsthand experience with the challenges of providing physical security in a city known around the world for its distinct public spaces. Our commission understands that access to our government, as well as the important public spaces that define our Nation's capital is worthy of our protection.

NCPC is concerned about the continuing challenges of balancing security and accessibility. Over the past decade we have worked hard to minimize the impacts that physical security measures have

on the public spaces that define the city and represent our democratic values.

In response to the unsightly security futures erected in Washington, D.C. After the tragic 1995 bombing in Oklahoma City, NCPC prepared and adopted *Designing for Security in the Nation's Capital*. Released in 2001, this report identified an approach to designing future security features in Washington that would reduce their impact on public spaces.

Following 9/11, NCPC published the National Capital Urban Design and Security Plan in October of 2002. This plan provided physical guidance for the design of contextually sensitive physical security features appropriate for use in the monumental core of the city.

In our review capacity, NCPC has regularly worked with applicant agencies over the past 10 years to reduce the impacts of proposed security improvements on the environment and public space. For example, NCPC was instrumental in guiding development of the landscape security solution on the Washington Monument grounds that is widely praised as successfully marrying landscape amenities and improved security.

And most recently, in 2008, NCPC assembled a security task force to address the impacts that security projects were continuing to have both individually and cumulatively on the city's important public spaces. The task force included members of our commission, but also included participation from government security professionals, including the Department of Homeland Security and the United States Secret Service.

Through this 1 year effort, NCPC's security task force reached several conclusions regarding the challenges of physical security. It also developed alternatives to better balance the need for security with the value of providing and maintaining openness in the Nation's capital.

The security task force found that, one, because the probability of any specific type of attack on a facility is so difficult to quantify, the current determination of risk is based primarily on the vulnerability of a facility and the potential consequences of an attack. This approach to assessing risk often leads to proposals for extremely robust security solutions.

Two, that existing security standards may seem appropriate in cities with only a few facilities that need protection. But these standards which are focused on increasing protection and physical standoff at individual facilities are more challenging in cities with many assets such as Washington, DC.

Three, because individual Federal agencies are responsible for securing only their individual facilities, area wide security improvements that could benefit the entire city or monumental core are less likely to be identified and implemented.

And four, security proposals for individual buildings are often developed specifically to satisfy existing security standards, not balancing improved security against other public or environmental impacts.

NCPC's security task force determined that bringing together the views of planners, designers, security professionals, Federal landholding agencies and Federal and local oversight agencies to guide

the planning and development of future security improvements can help meet these challenges. These groups need to work together to, one, prioritize security improvements at Federal facilities; two, identify the most cost efficient way to address our most critical security needs; and three, coordinate future security improvements to make sure that they address and respect the needs of Federal and local facilities in the city; and finally, four, ensure that individual and cumulative impacts to public space, public access and the environment, are fully considered before implementing physical security projects in the future.

While it is important to make sure that we protect our Nation's most valuable assets, we must do so in a way that considers the impacts of our actions and which does not unduly harm the public spaces or the public access to our government.

Thank you for inviting me to share NCPC's perspective on the challenging work to balance the need for improved physical security with the potential impacts that physical security projects have on public spaces and access to our government. We would be happy to answer any questions following the panel.

Ms. NORTON. Thank you, Mr. Dowd.

Next we will hear from Gary Schenkel, Director, Federal Protective Service, which is a part of the U.S. Immigration and Customs Enforcement. Mr. Schenkel.

Mr. SCHENKEL. Chairwoman Norton, thank you for this opportunity to appear before you today to discuss FPS mission, risk-based security in Federal buildings, as well as describing the steps we have taken to address the concerns raised by the Government Accountability Office.

As you know, to serve customer agencies in Federal facilities, FPS must effectively balance the need for security with the need for ready public access to government services. This means that FPS, in conjunction with the agencies that occupy the facilities, must provide security solutions and ensure safe and secure environments that do not deter people from conducting regular business. FPS offers comprehensive physical security operations, installs security systems, alarms, x-rays, magnetometers, entry control systems, monitors those systems 24 hours a day, 7 days a week, and provides uniform police response and investigative follow-up. The provision of contract security guard services crime prevention seminars tailored to individual agency and employee needs, facility security surveys, integrated intelligence gathering and sharing, and special operations capabilities are all part of the broad FPS mission.

Upon my arrival in 2007, it was apparent FPS was experiencing some challenges. The agency transferred from GSA to DHS in 2003 with a full-time equivalent work force of over 1,400 spread across the country in 11 different regions. And I saw that FPS needed to focus on becoming a single standardized organization. This required a new operational construct and new business practices. However, FPS simultaneously faced budget constraints due, in part, to poor financial and contract management, as well as fee collection, requested in the President's fiscal year 2008 budget that supported fewer personnel than we had on board and at the time the budget was sent to Congress. To avoid having to reduce the

numbers of Federal employees, FPS sought to realize savings in other areas.

Consequently, many programmatic elements, such as training and equipment purchases had to be rescheduled until such time that FPS could determine it had sufficient funding. FPS of course remained obligated and dedicated to protect the almost 9,000 GSA owned and leased facilities and overseeing 15,000 armed contract security guards and managing over 150 contracts.

During this period, FPS carefully assessed its organization and made difficult decisions. This refocusing effort culminated in the development of a strategic plan to shape future activities. FPS now focuses on critical issues within its protective mission and is developing a sound strategic path forward focused on facility security and the safety of the occupants and of the visitors who visit those facilities.

With respect to the GAO report released in July, we took many steps to improve the visitor and employee screening process at Federal facilities, including improved training of contract guards and oversights of those guards. In addition, I believe that more work is needed to improve the training of contract guards and additional study is required to determine whether contract guards are maintaining constant vigilance. To that end, FPS is taking steps to bolster training and performance, increase oversight and supervision and create a more uniform protective system. After reviewing the problems identified by the GAO, I believe that the steps we have taken will redress these problems and the proposed future steps will ensure the improved protection of nearly 9,000 GSA owned and leased facilities protected by the FPS work force and our contract guards.

I think it is important to note that FPS has limited authority with regard to the 9,000 or so facilities it protects. Although responsible for securing the facilities, FPS cannot set standards or require a particular facility to have the best available security equipment. Instead, building tenants make those decisions. Each building facilities security committee, or FSC, makes the final determination on the facilities security level and sets the building's access and security policies.

Thus, FPS, although expert in physical security, faces challenges in protecting facilities and their occupants as FPS may deem appropriate. Tenants may select security controls and options that FPS' physical security experts have neither recommended nor endorsed. The GAO reported recently that only 12 percent of the leaders of these FSCs have any security experience.

Chairwoman Norton, I applaud your leadership role and the effort to strike the right balance between security and access to our Federal buildings, and look forward to working with you and this Subcommittee on addressing those challenges. I want to express to you my personal sense of urgency and commitment to the important responsibility I share with the men and women of the Federal Protective Service in keeping our Nation safe. I can tell you that they, as are Secretary Napolitano and Assistant Secretary Morton, are dedicated, determined and committed to developing, implementing and maintaining the highest level of physical security to

ensure that the facilities they are charged with protecting are secure and their occupants are safe.

I thank you again, Chairwoman Norton, for holding this important oversight hearing. I will be pleased to answer any questions you may have.

Ms. NORTON. Thank you very much, Mr. Schenkel.

Mr. Patrick Moses, the Regional Director for the National Capital Region of the FPS. Mr. Moses.

Mr. MOSES. Chairwoman Norton, thank you for the invitation to appear before you today. I currently serve as the Regional Director of the National Capital Region of the Federal Protective Service. I was appointed to this position in September 2008, and I have served in the Federal Protective Service for 14 years.

As part of my responsibilities I direct the regionwide infrastructure protection program by mitigating risk to Federal facilities and the occupants for 772 facilities operated by the General Services Administration, including a number of high profile facilities such as the Ronald Reagan Building and International Trade Center and the Nebraska Avenue Complex.

Since Director Schenkel has provided the Subcommittee with a written statement on behalf of the Federal Protective Service, I will forego making a formal statement at this time, but will be happy to answer any questions.

Thank you.

Ms. NORTON. Thank you, Mr. Moses.

Mr. Peck, Mr. Porcari cites, page 2 of his testimony, based on a delegation of authority provided by the Department of Homeland Security through the Federal Protective Service, the Secretary of Transportation is solely responsible, without limitation, for protecting the DOT.

Should GSA be delegating authority to agencies to set up security? Agencies like the Department of Transportation don't have a smidgeon of expertise on security of the kind we are talking about here. Should that be the practice? I am not asking you. I know you weren't there. Most of you at this table weren't there, and that is why I am looking less for apologies than I am for people who would want to take on this unprecedented activity with me. But I am asking, as a matter of practice, should the agency be delegating such security authority to an agency regardless of its background or expertise in security?

Mr. PECK. My short answer is no. You know, for 20 some years we have delegated the management of major Federal headquarters buildings, mostly in Washington, to the agencies. And I suspect—

Ms. NORTON. You know, I can understand certain kinds of management notions being delegated. So, no, I accept that. We are not trying to, you know, centralize everything. I serve on the Homeland Security Committee and they have centralized the world in Homeland Security in order to protect us. So I accept what you are saying.

Go ahead.

Mr. PECK. Correct. And what I was going to say is I just suspect that since when that program first came in, I think building security was considered an aspect of building management. That has probably been the way delegations have happened. What I am tell-

ing you now is I think that we should reconsider whether that is a part of a delegation to an agency.

What is important, of course, is that we consult with the agencies, because only the agencies can know how they actually use a building and what they need and what kinds of visitors they have and what requirements they have on deliveries and loading and all those things.

But, again, as I suggested in my testimony, and I think you hear from Director Schenkel's also, that the balance of responsibility, of decision making about security in buildings is probably something that we ought to move back a little bit more, maybe even a lot more, toward those who have the security expertise.

Ms. NORTON. Do you agree, Mr. Goldstein? You, who are an expert from the GAO, where should the responsibility lie? Should it be with the HHS? Should it be with the Department of Education? Should it be with the Department of Transportation? Or is there some authority that is specialized enough within the Federal Government to advise agencies in consultation with them about our security for millions of Americans and Federal employees?

Mr. GOLDSTEIN. We have not looked at the question specifically. But I would have to say in the work that we have done examining FPS and Homeland Security and some other agencies as well, it seems to us that some greater centralization, as you say, with consultation is probably useful at this point in time. The whole building security committee apparatus, the way in which risk management is approached as well, does not provide an avenue for GSA and FPS to look at the entire portfolio of Federal buildings and determine where the risks truly lie and how to protect them in a risk-based case.

Ms. NORTON. Isn't there a difference between some buildings and other buildings in the GSA inventory?

Mr. GOLDSTEIN. Yes, ma'am. Absolutely. Even, you know, while there is currently under the standards a level I through V category distinction that separates risk—

Ms. NORTON. Because most cabinet agencies will be at least level IV, won't they?

Mr. GOLDSTEIN. Most, certainly their headquarters buildings will be, absolutely.

Ms. NORTON. So we understand we are all high level. We are all very important. And we think that if some have higher level security than others it is not because they are more important; it is because terrorists and other criminals may seek access to those buildings more often than to others.

Mr. GOLDSTEIN. That is correct. And one of the issues there is that the Federal Protective Service historically has not had great access to threat information and also does not have terribly useful crime statistics coming out of its own mega centers to help to determine where those greater risks lie.

Ms. NORTON. Say that again. I am sorry. You know, I can't always understand you.

Mr. GOLDSTEIN. Sure. Two points I was making. One is the Federal Protective Service has not always had great access to threat information from the Joint Terrorism Task Force.

Ms. NORTON. What do you mean? They are part of the Homeland Security Department.

Mr. GOLDSTEIN. That is correct. But in the conduct of our audits over the last couple of years, we had many FPS officers and officials out in the regions tells us that their access to Joint Terrorism Task Force information was very limited.

Ms. NORTON. Do you need access to Joint Terrorism Task Force information to do what was done at the Ronald Reagan Building by the private sector, working with the FPS?

Mr. GOLDSTEIN. I can't answer that question. What I am suggesting—

Ms. NORTON. I guess it is a rhetorical question.

Mr. GOLDSTEIN. They do lack significant information that they would need to develop a better risk-based model—

Ms. NORTON. I question that, Mr. Goldstein. I really question that because we gave very detailed questions to the witnesses that preceded you and they didn't anymore have expertise and background than the FPS before, for that matter, Oklahoma City. Nobody knew how to do this. But they were given a mandate by statute, and that was to make this building private to the greatest degree possible and FPS, you better make sure that the public part of it is as safe and secure as need be.

And I guess I should ask if anyone else at the table thinks that there has been difficulty figuring that out without access to the highest level information, because the next thing we are going to hear, Mr. Goldstein, is unless we know all the threat information that the Secretary knows, don't expect us to be able to guard these buildings in the way you want.

But, I mean, you all didn't have that at Ronald Reagan. And yet you have got a million visitors coming to Ronald Reagan. And the highest profile building outside of the Capitol and the monuments and the White House, and the President can go in there today and I am not sure who has access to all that highly classified information.

So I hear you, Mr. Goldstein. Mr. Peck.

Mr. PECK. Well, let me see if I can make a distinction. The point in the Ronald Reagan, which is, by the way, a great example of how you can get the tenant agencies and a private vendor and FPS and GSA to work together on this. However, is that the Ronald Reagan, we assume, is a very high risk target and we have had protocols developed with the Secret Service. Whether FPS has access to the information now or not I don't know. I know they did have trouble at one point in time.

Ms. NORTON. Well, FPS doesn't need to if it is in consultation with people who do have access and they are acting reasonably.

Mr. PECK. That is correct. And on the Ronald Reagan Building since we assume it is very high risk, we assume that we need a very high level and we have been able to assume that. I think the issue becomes a little bit more important, what Mr. Goldstein is talking about, where we have buildings that are probably in a lower risk category, and there we need to have the people—our tenants need to have the confidence that FPS knows what it is talking about when it sets a risk level because if we are—may I just say one other thing. You put your finger on something before. That if

a facility security committee run by people who aren't security experts, don't know what the risk is, don't know what the best practices are, they are going to naturally go to the highest level of security that they have seen in some other building. To be able to convince them that in some buildings we don't need things ratcheted up that high, they need to have confidence in us that we know what the risks are, we know what the proper countermeasures are.

Ms. NORTON. That point is very well taken. And yet, Mr. Peck, it looks like the GSA or the FPS is buried when it comes to security. We have got something called the Interagency Security Committee, ISC. Now, you are the only agency who has the mission of managing, you are the PBS of managing property. So far as I know, you are neither Chair, you of the GSA or of the Federal Protective Service, either Chair or even have a particular leadership position. I don't even know, maybe Mr. Goldstein or somebody knows, whether your even being at the table matters. Who is in charge of this committee?

Mr. PECK. Well, I think Homeland Security is chairing the ISC at the moment.

Ms. NORTON. Who? Who is that? What agency? Is there a Chair?

Mr. SCHENKEL. Madam Chairwoman, the Assistant Secretary for Infrastructure Protection is the actual Chair of the ISC.

Ms. NORTON. Assistant Secretary for—

Mr. SCHENKEL. Infrastructure Protection.

Ms. NORTON. And of course, Mr. Schenkel, you don't even come under that division.

Mr. SCHENKEL. No, ma'am. No, ma'am.

Mr. PECK. If I may say, one of the problems—

Ms. NORTON. So that is the—and everybody else is kind of at the table; is that it, Mr. Schenkel?

Mr. SCHENKEL. It is, I think it is a group of 24 members, actual voting members. Everyone has access to the meetings and certainly has to abide by the decisions.

Ms. NORTON. Where are their decisions published?

Mr. SCHENKEL. They are published in their own directives that they put out at the facility's security level.

Ms. NORTON. Could you get to this Committee within 30 days their directives that all agencies under their jurisdiction must apparently use this guidance? Mr. Peck.

Mr. PECK. May I just say, at least, when I was in the private sector, a good number of the ISC criteria are actually on-line. They are not classified. So they do have them. Can I just say though—

Ms. NORTON. Mr. Schenkel, would you get to us within 30 days the material on-line or off-line and tell us whether it is agency wide so that we may see what guidance the agencies have been given?

Mr. SCHENKEL. Yes, ma'am.

Ms. NORTON. Now, everyone at the table should know that we are not here to say why haven't you done X, Y, or Z, or why did you do X, Y, or Z. We know the reason. We do not believe, despite whatever is on-line, that the agencies consider that there is an authority, nor has Mr. Goldstein testified to any authority that agencies look to. So I am not saying how come you are doing this, that or the other. I believe the agencies are doing the best within their discretion. I also understand that not everybody has been at the

table the whole time. Some had to be at the table to make it up as they went along. That is how—that is what we are doing right now. We are just trying to see if there is a better way to do it. So I would caution everybody, since I am not holding those who put it in place without guidance or sufficient guidance responsible, I don't think anybody at the table at all ought to put that monkey on your back because then you are going to own it if you want to, in fact, use it as the reason for what you are doing.

And I say that to you, Mr. Porcari, because I don't believe you have testified before us. But you did say, quite truthfully, I have cited it to Mr. Peck, that you are doing what has been delegated to you. But on page 2 of your testimony, you also said that the DOT headquarters security was developed, and you go on, and a detailed risk assessment analysis conducted specifically for the Department that validated our requirements were appropriate for a cabinet agency with mission essential functions.

Now, mind you, I know fully what your mission is. This Committee is part of the Department of Transportation and Infrastructure, and I am on the Homeland Security Committee, so I am not in doubt what your mission is. And your mission is very important to the United States. But let me tell you and ask you whether you think this can be improved. You heard Ms. McCann testify about what I think could be called arbitrary treatment. Some guards let you take pictures. Some guards don't let you take pick pictures. And she said, she quoted a 2004 Mr. Schenkel security bulletin regarding photography at Federal buildings. And this is what she quoted from a 2004 Homeland Security bulletin that was apparently published right here for the public to read.

Widely known reconnaissance activity of criminal and terrorist organization has been—I am sorry. Claiming, the document claimed that a widely known reconnaissance activity of criminal and terrorist organizations has been to gather photographic information about prospective targets.

Agreed. Do you think it is appropriate today for the Department of Homeland Security to keep a citizen from taking a picture or that you are endangered if somebody takes a picture of the front or the back or the side of the Department of Transportation headquarters?

Mr. PORCARI. Madam Chairman, let me first apologize to Ms. McCann. I know that we did respond in writing. That action was inappropriate. We said so at the time. I just want to reiterate that personally.

Ms. NORTON. Thank you for that.

Mr. PORCARI. And the November 10, 2004, Federal Protective Service bulletin is what we have been following. And I would also add that we have, since that incident, given written guidance to the security personnel at the building that references that and that is very specific about how they should be.

Ms. NORTON. Saying what? Would you just characterize how, because you know what happens? And I warn you. People who brought this to our attention were young people. They are going to start snapping the pictures left and right.

Mr. PORCARI. I do understand.

Ms. NORTON. And you are presumed to be under oath here. We don't, and I may have to do this. I may, you know every other Committee they make people stand up. I exercise a presumption in favor of the truthfulness of anybody who appears before me. So be careful about your answers. They will test you out.

Mr. PORCARI. You should be able to rely on that assumption in the roles that we are in. That is an explicit part of the job.

Let me just characterize some of the important points that is in that guidance. It says first please understand there is no prohibition against photographing the DOT or FAA headquarters buildings. Second, however, because reconnaissance activity of criminal and terrorist organizations has been to gather photographic information about prospective targets, security personnel should follow the procedures. That wording is directly from the Federal Protective Service 2004—

Ms. NORTON. That is good. So far so good.

Mr. PORCARI. One, approach anyone within DOT or FAA boundaries taking photographs of the building and identify yourself. In other words, as a security officer. Two, conduct a field interview to determine the purpose for taking photographs of the facility and endeavor to ascertain the identity of the individual. That, again, is wording directly from the FPS 2004 guidance. If the field interview does not yield a belief of criminal behavior or terrorist reconnaissance activity, the photography should be permitted without further action.

Ms. NORTON. What is going to happen, Mr. Porcari and Mr. Schenkel and Mr. Peck, as you can see from Ms. McCann, I don't even know if she is a lawyer. All I know is she is typical of the people I represent. Smart. So I am going to have to ask you, does that directive apply, if you are taking pictures on the property or if you are taking pictures a few feet back from the property?

Mr. PORCARI. This applies, to my knowledge, on the property. The property extends to the curb line.

Ms. NORTON. So, I understand, and I understand, Mr. Porcari, you are quoting from what the directive says. And you are abiding by the directive. And Mr. Goldstein, that is why I believe security isn't worth a tinker's damn, if you will forgive the expression, because I believe you can get a better reconnaissance picture of DOT by getting across the street and using one of the new-fangled or for that matter old-fashioned cameras. And I think you could get something that would be virtually like a blowup of every part of it. And yet, Mr. Porcari, according to the guidance he has, has got people who could be looking for some people who are trying to get into the buildings, going up to American citizens and questioning them about what they are doing there.

Now, I say, and putting on my old hat as a constitutional lawyer who has argued before the Supreme Court of the United States, I say that there is a serious risk, and we have already seen Union Station, inside the Union Station, they understood you had better not do that. There is a serious risk to go up to a law abiding person who is exercising her first amendment rights to take a picture of the building she owns as a taxpayer, and interrogate her to make sure who she is, unless there is a risk that can be demonstrated.

I have just tried to give you the kind of law school hypothetical I use still as a tenured professor of law at Georgetown University. I say to you that not only have I found it difficult to see the risk, but it is far from, not only is there no overriding risk to infringe upon the first amendment right of the citizen, I believe the terrorist is better able to take pictures off the property and that no U.S. attorney would do anything if a suit was brought but give up. That is just how off the mark, given the so-called preferred rights, first amendment rights are, and I am denominating the right to take a picture as a first amendment right.

So I am trying to find out whether or not what is printed out so that Mr. Porcari is only following the directives that Mr. Schenkel and Mr. Peck's organizations have said he should follow, I am asking you, as security expert, whether or not you believe that a justification can be, and ask you to stretch now and help them out because they could find themselves in court. Is there a justification that could be made for keeping somebody on Federal property where you have a right to be because it is Federal property which itself is not off limits as secure property, is there, could you argue that it is justified to begin interrogation of a citizen taking pictures?

Mr. GOLDSTEIN. We have certainly not looked at the issue in any of its facets, Madam Chairman. I would say though that many of the policies that FPS promulgates are not enforced in any kind of uniform standard, and that is part of the problem that you do face even with those standards that ought to be enforced, no less those that may have some questions about whether they should be enforced or not.

Ms. NORTON. So we are looking for, to help the agencies get some kind of guidance to take seriously. Now obviously some don't take it seriously at all. The testimony was that DOT doesn't take it seriously some of the time and take it seriously—in other words, the guard in his discretion can see silliness of this perhaps and say I am not going to let that come out of my mouth that you better not take pictures, so maybe he lets it go. Another guard says I am by the book so I do it. That is where risk comes in, where you have that kind of inconsistency.

But, Mr. Porcari, I am going to tell you about an experience we had. Let me first thank you on behalf of and ask that you thank those at DOT who have been very kind to us. We have had, we have been into your courtyard, we love it, where you are good enough to have a farmer's market if you still do. Certainly you did.

Mr. PORCARI. We do.

Ms. NORTON. We have had events, as you indicated, in your building. But let me tell you what has not changed. You work very closely with the business community in your area and this applies to them as well as to others. When we first went to use this beautiful facility which came through this Committee, I might add, my staff, staff of the United States Congress, which have this ID around them, were not allowed, who have a higher, I would argue, security clearance than most in your building, were not allowed to enter the building even with their ID and even after a magnetometer. So somebody, they were told, from the building had to come down and let them in. And the same way we are informed

by people who actually work with you on a cooperative basis, because DOT has done very good work in working on the M Street corridor, with those agencies and private entities, that even they, people in the business community, in the local BID, what do you call it, the BID, Business Improvement District, were required to get an escort to get into the building from the courtyard. When we held an event there, while there were people stationed at various doors, we were told that if they happen to come from another area they could only enter from the other door until I personally intervened since the door they were supposed to enter into was the furthest from where the event was being held. The guards were only doing what they were supposed to do, but it was an exasperating and frustrating experience, and the DOT became the poster child in one sense, for this hearing when we saw that people who had passed the highest security even in the Congress of the United States couldn't get in the building. And people with whom you were familiar couldn't get in the building unless somebody came down and escorted them into the building. And who knows, that might be a different person each time, for that person was pulled out of her work in order to come down to do what the magnetometer or the guards could do.

This is what I mean by make work, and I need to know whether you are prepared to look closely at the DOT building in particular and to make sure that it does what page three of your testimony says, overall the security practices and policies of the Department's headquarters building are equivalent to other cabinet agency headquarters in Washington, DC.

Nonsense. You heard Ronald Reagan, which has cabinet agencies, you heard the testimony there. I know of no—I can tell you that I know of no agency, perhaps the CIA, where it is harder to get into than the Department of Transportation. And while people may try to get to parts of your agency over which you have jurisdiction, and trains and airports, we do not believe that your headquarters are nearly as high profile a target as many headquarters in Washington, which are identifiably higher terrorist targets.

So I am not asking you to justify it. You weren't here. But you do say that you meet—you do what others do. I don't know anybody else who pulls people out of their work to come down in order to escort people in. I don't know anybody else where you can't use the john and you have a kid and you say, but isn't this a Federal building? I know very few Federal buildings where you can't get in to do a restaurant. I tell you one thing. Mr. Porcari, you can get into the Reagan Building, Longworth Building, and Cannon building in order to use our facilities and in order to go to the restaurant. You can get into the Capitol of the United States across the street in order to use the facilities. How are we able to allow the DOT to continue to have a stricter protocol than in the building where you are now sitting?

And all I am asking you to do is not to justify. God help you if you are going to justify it. I am asking you, are you willing to look at it so that we do not have testimony that says you are equivalent to other buildings, when this Member of Congress has entered other buildings and had staff members enter other buildings and

have them enter this building and know firsthand that it is not equivalent to other buildings. That is all I am asking.

Mr. PORCARI. Madam Chairman, a couple of things. First, you started your opening statement by making what I think is a very important point, which is this is an issue of balance and that balance is different given the circumstances and the particulars of it. I think that is certainly true in the case of the DOT headquarters building. You are correct.

Ms. NORTON. Excuse me. And how—why is it balanced? You can't just make a blanket statement like that.

Mr. PORCARI. I am trying to get to that.

Ms. NORTON. Okay.

Mr. PORCARI. An escort is required in the building and it is a function of the building design. It is fundamentally an open office environment. When you go through the security, past the magnetometers, you can go anywhere, unfettered access to the building. It is a building that also has—

Ms. NORTON. That is the case in every building, sir. Once you get through the magnetometers here, guess what? You can go, you can get to the Speaker's office. You can go through the tunnel because once you have come through Rayburn, you now have access to all of us. So I want to know why that puts you in a different position than it puts me.

Mr. PORCARI. This security procedure was set up at the time based on an open office environment and some of the functions that are within it, including the crisis management center which is opposite the cafeteria on the first floor of the East Building, including the SCIF facilities that are in the building. And—

Ms. NORTON. I know exactly how this was built. It took me 10 years to get the darn building up. Frankly, I don't like the building very much. But I don't like the architecture in my hometown very much, and I am a third generation Washingtonian. If I had to start, I would blow up the place, give it to Mr. Dowd and say, let's start all over again. But these buildings are built within the security constraints and particularly within the budget constraints. So we are going to be building more buildings like that.

Are you testifying that the only way to do business in an open office environment is to pull people off their work every time somebody comes down and wants to use the john in the building?

Mr. PORCARI. No, I am testifying that that is why it was set up that way, with an escort required because of the open office environment function.

Ms. NORTON. Well, is it still set up that way?

Mr. PORCARI. It is still set up that way.

Ms. NORTON. You don't have to justify what happened. I don't justify what my predecessor did, nor do I throw him under the bus. That was then. I am trying not to look backwards. I am trying to be prospective. Now, if you want to take that burden on, Mr. Porcari, you take it on. I understand what happened in the past. I am trying to see if we can make things better now.

Mr. PORCARI. Madam Chairman, about 110 days ago when I was in a different role I had a very different perspective of this, including what these security procedures mean for mixed use transit oriented development, the need to mix both governmental functions

and other functions like the Reagan Building does with the food court and the other public portions of it. I would, again, go back to the balanced part of it. I am not going to tell you today that we have that balance perspective because I am not sure that that is true. And it certainly changes over time.

Ms. NORTON. Mr. Porcari, and of course I am not asking anybody that. I started this question off I think the right way. I asked you were you willing to look at the current procedures, not whether or not you had it right. It wasn't yours in the first place. It wasn't even the people at DOT in the first place. They got it out of the guidance and, you know, Mr. Schenkel doesn't know who in the hell that guidance came from, for that matter.

Mr. PORCARI. Working with FPS, GSA and others, we are very happy to look at those procedures. One of the points I was trying to make is that this, none of this is static. I don't think anyone believes that a process that you set up at a point in time would be the most valid one forever.

Ms. NORTON. Forever is a long time.

Mr. PORCARI. Absolutely.

Ms. NORTON. And you will find that this Committee is only looking for what human beings can do in the short term. That is why I ask for a review and why I get impatient if people are not willing to go through the same head process I am going through. I don't know what you should do. I also believe that building by building is very different. I have given you examples of practices that you have not attempted to justify, and I think that is appropriate. I am only asking since you are a new regime, if you will forgive me, if you would be willing to look at things like whether or not a taxpayer, finding herself with her kid on M Street, which is still being fleshed out, could enter the building to use the facilities and whether or not you might think through a way to do that, whether or not, in one of the few eating places on the whole of M Street, it might be, it might be possible to open that cafeteria to people who will not find restaurants yet on M Street, but will find a building that costs them billions of dollars to build. I am asking you if you are willing to do that. And all I need is a straight answer on that.

Mr. PORCARI. The answer is yes. And I have—

Ms. NORTON. That is all I need, sir. And I ask you within 30 days to give this Committee not what the answer is, but what your procedure will be for looking at the examples I have given you and others that your security people will tell you, the example from Ms. McCann. I need to know what training you intend to do to the guards so that they are consistent. I need to know what the training is now that is already written someplace. And I need to know how you intend to consult in order to revise, if necessary, current procedures. Let me just warn people. Don't make—I am outraged at what has happened, but I am not your adversary unless you want me to be one. And I know how to do that. And I certainly don't expect Mr. Porcari says, you know, you expect things to change over time. Mr. Porcari, 8 years after 9/11 we are still using many of the procedures that we used on day one on 9/11.

That is from whence cometh my frustration. If you had sat where I sat and saw the streets closed up, and it took me months to get the streets opened up, largely because people didn't know what to

do. And I don't know what to do. If you live in a continental country, surrounded by water on each side, you have no reason to know what to do until you were hit on your own soil.

So we don't have to be apologetic for that. We just have to do, and here I go to Mr. Dowd. The NCPC has been very forward looking and thinking, maybe because it didn't have to do the security. But that is why we need them. But NCPC has been important to us because they look at best practices. We believe we are not asking the Federal Government to do what Europe hasn't learned to do. We are very fortunate. We haven't been struck. When we are struck we are struck very mightily. But if you go to the capitals of Europe, you want to see struck, go to the European countries and you will see spectacular, spectacular threats, risks and actual strikes.

I am going to ask Mr. Dowd, because one of the things this Committee is going to do is to try to better incorporate your work as administrative agency into the work of our agencies. Are you aware of best practices for building security in major, I don't know, European capitals that work any better than what appears to be ad hoc approaches here?

Mr. DOWD. I can share some of the information, Madam Chairman, that we have. We held a workshop last July and we invited some other countries. Actually England came and spoke with us. And one of the things that they do there is it is more of a layered approach to security. They pointed out that in our country we have a lot of assets and we invest heavily in trying to protect them all. And they felt that we were rich and we are able to make those larger investments. But they struggle more with how do they do more with less to protect the assets they have. One of the approaches that they identified was in London, their ring of steel, which is a circumferential border around downtown London where they check license plates and have license plate recognition and sort of meter the traffic in. And they can identify if vehicles of threat are approaching the city.

Now, that is not the only way to address physical security. I guess—let me back up. Our approach was really just on physical security, so I respect there are many other aspects of security that each individual agency protects. But as you know, our commission's purview is on the physical aspects. But we did learn that there are other approaches to doing that. And like I said, in London they looked at a layered approach where they tried to manage security for the entire area and then for their most critical assets, which they prioritized, provide additional physical security at that site.

We are hopeful that we can learn from some of those experiences as we introduce security here in the monumental core. Domestically we have a similar approach in New York City, the Lower Manhattan Security Initiative, where they have limited access points to Lower Manhattan and approaches like that work. It will be a little bit more of a struggle here, but we can clearly learn from those lessons.

Ms. NORTON. Very limited approaches anywhere in downtown Washington, sir. The whole city is limited. I ask because we always have to tailor what we learn elsewhere, but those places at least have the experience of being far closer to places where the risks

exist. And I don't expect that you will have any particular model that fits perfectly.

Let me ask, I guess, Mr. Goldstein, Mr. Peck, Mr. Schenkel, about the fee for service approach to Federal Protective Service because we realize that funds have been at the core of many of the FPS problems. That is one reason it would appear that they decided to get out of the protection business altogether and just inspect things, don't do proactive patrols, which if you want to prevent terrorism I thought was one of the standard ways to do it. So we are not laying all of this at your feet. We ourselves, for example, Mr. Schenkel, had to request a minimum number of FPS officers. By the way, is that minimum number, Mr. Goldstein or Mr. Schenkel, still enforced?

Mr. SCHENKEL. Yes, ma'am, it is.

Ms. NORTON. But here you needed the authorizing and appropriation Committee, because the agency was being literally drained of personnel. So again, I stress, I am not laying this at the feet of the people at the table, but unless we find out what the facts are, we won't be able to be of any help.

Now, the fee for service based financing, I take it, does not take into account things like square footage, like Mr. Porcari has a very large facility now. Does it? How does fee for service work? How do you even decide what service you ought to have if you have got agencies that contrast in size the way our agencies do?

Mr. SCHENKEL. Madam Chairman, we are not fee for service, but we are fee funded. And it is basically—

Ms. NORTON. So what is the difference?

Mr. SCHENKEL. You get the same service, the formulation put together is actually based on some of the facilities services that we provide. The square footage is just a basic security fee which is the presumption that you would receive some basic functions from the FPS.

Ms. NORTON. Well, between the three of you, you have got to make me understand how do we decide how many FPS agencies Mr. Porcari ought to have and HHS ought to have? If it is not fee for service, if it is something else, as Mr. Schenkel says, it is fee, if it is not square footage, then please make me understand what it is that—

Mr. GOLDSTEIN. Madam Chairman, it is at \$0.66 per square foot, which is charged to all the tenants in the Federal buildings that FPS protects.

Ms. NORTON. So it is square footage.

Mr. GOLDSTEIN. Yes, ma'am.

Ms. NORTON. So is that a rational basis then for doing it? Is it based on size then? The more square footage? The more what?

Mr. GOLDSTEIN. Well, regardless of, one of the things we have been concerned about, and we wrote in our last report to you last July we have been very concerned about this approach because regardless of whether you are located in a level I facility or whether you are located in a level IV facility, whether you have FPS officers who visit you and are with you virtually all the time, or whether you don't see them for 6 months, you have to pay the same amount.

Ms. NORTON. That would be based on what? Whether they visit you often or not would be based on what today?

Mr. GOLDSTEIN. Whether they are anywhere near you. In other words, if you are a level I facility in Iowa, or you are a level IV facility in Manhattan, you are still paying \$0.66 per square foot. If you are in Manhattan you are likely to see FPS officers pretty frequently because most of them are urban based. There is more in urban areas because FPS has decided based on its risk management approach that that is where most of its officers would be. But you are still going to pay the same amount of money.

Ms. NORTON. Let me understand. Because, you know, per square foot makes some sense. But are you saying that it is not risk based per square foot?

Mr. GOLDSTEIN. That is correct. One of the problems we have is there is no equity in the situation. Everyone is paying the same amount.

Ms. NORTON. So I could be where terrorists were given to believe, based on the intelligence before me as a Member of the Homeland Security Committee, I could be in some place in a rural area which maybe because it is in a rural area has a particularly large Federal facility, but that facility houses agencies that have never been considered targets for terrorists but because it is a large facility for efficiency purposes, it could receive more FPS coverage than say a smaller square foot facility that is more highly targeted?

Mr. GOLDSTEIN. That is correct. In our report last year to you, ma'am, we recommended that FPS improve the use of the fee system by developing a method to accurately account for the cost of providing for security services and to evaluate whether the current use of the system made sense or whether they should develop an alternative funding mechanism. But those recommendations, along with other recommendations in that report, have not been closed yet. They have not reported back yet.

Ms. NORTON. Well, you state at page 2 of your testimony, Mr. Goldstein, that FPS does not use a risk management approach. Your words, a risk management approach that links threats and vulnerabilities to resource requirements.

What approach do they use?

Mr. GOLDSTEIN. That is correct. They mainly use the building security assessment process to determine what the risks are in their view on a building-by-building approach. But as you know, we have reported about problems about the building security assessment program itself over, in our report.

Ms. NORTON. So what is the problem with the building assessment if they are looking at it building by building?

Mr. GOLDSTEIN. Well, there are specific problems with how they are doing the assessments. And then more broadly there are problems with doing it on a building-by-building approach as opposed to assessing risk across the portfolio.

Ms. NORTON. So if they assess risks across the board, wouldn't they also have to do some building-by-building assessments?

Mr. GOLDSTEIN. You would certainly have to do some building by building assessment, but the tools they have do not let them compare the risks across the buildings today.

Ms. NORTON. Would you consider the Department of Transportation a high risk facility for terrorist attack?

Mr. GOLDSTEIN. I have not looked specifically at that. I couldn't answer the question, ma'am. I mean, obviously their headquarters building. I presume is a level IV because it is a headquarters building.

Ms. NORTON. So every level IV facility is equally a target for terrorist attacks?

Mr. GOLDSTEIN. Well, that is, I think, part of the issue that I am trying to raise. It is equally categorized in terms of risk, but every level IV building in the Federal portfolio may not have the same level of risk associated with it.

Ms. NORTON. Are the buildings, in fact, characterized in terms of actual risk based on function?

Mr. GOLDSTEIN. Not really. It is mainly in terms of size of building, the numbers of employees in those buildings, generally speaking, the kinds of agencies inhabiting those building. It is not specifically based on risk.

Ms. NORTON. It sounds like you need a new matrix or grid in the first place to look at buildings so that agencies aren't—

Mr. GOLDSTEIN. The new security standards that have been promulgated but are not in effect yet go further than the old Department of Justice standards.

Ms. NORTON. Promulgated by whom?

Mr. GOLDSTEIN. By the Interagency Security Committee. They go further than the old Department of Justice standards in trying to establish some risk parameters, but it is still questionable as to whether they go far enough and it may be something we should look at at some point.

Ms. NORTON. Mr. Peck.

Mr. PECK. Yes, ma'am. I don't want one of Mr. Dowd's points to get lost because it has a relationship to the whole—

Ms. NORTON. First of all, do you know anything about what Mr. Goldstein is talking about? There are some promulgated but not issued new—

Mr. PECK. Yes, the ISC has developed new physical security criteria.

Ms. NORTON. Do you have anything to do with those?

Mr. PECK. GSA has been on the committee that has been working on them and I—

Ms. NORTON. Should they be promulgated as they are right now?

Mr. PECK. They are still being worked out. There are some questions I gather about whether we have—within the administration about whether we have taken enough of a look at how much the criteria may cost in compared to how much more of a threat countermeasure they will provide. But they are on the way. I will say that I am told and I have to say, I haven't read them. I am told that they are more risk based than what we had seen before.

But you know, what Mr. Goldstein is getting to, and this is sort of the big question here is how do you measure risks? What are the risks by agency?

Let me make one point about the fee if I may. One of the problems with, and to defend FPS, I think what happened was we used to have a security fee tacked on to the rent that GSA charges. When FPS was taken out of GSA and put in Homeland Security, I think everyone said, well, we will fund them through a separate

little rent piece here. And I think it probably wouldn't be a bad idea to take a look at whether that makes sense because some of the inequity that we are talking about here will result. You get charged the same amount no matter how much stuff or people we are putting in the building for security.

But the other thing that that does is it discourages us to the extent this is a building by building security fee based system it discourages us from taking a look at the kinds of suggestions Mr. Dowd makes that you could create a security zone and not based on a building and you provide some of the building security by saying we are going to screen people someplace else.

So let me make two points about that. You see that system here on Capitol Hill. At the foot of Capitol Hill and elsewhere around, you will see Capitol police officers making sure that buses and big trucks don't get into this complex at all. That means that certain levels of security don't have to be borne by the building. And the same thing happens at the Ronald Reagan Building. Because we can screen trucks somewhere else we don't have to worry quite as much about getting them into the loading dock.

Ms. NORTON. Do you use that for other Federal buildings as well?

Mr. PECK. Pardon?

Ms. NORTON. Do you use what you are doing at the Ronald Reagan Building for trucks or other Federal buildings?

Mr. PECK. I am saying the trucks for the Ronald Reagan Building are screened.

Ms. NORTON. No, for other Federal buildings.

Mr. PECK. Oh, in this—

Ms. NORTON. Yeah, for the Department of Transportation trucks, for EPA trucks.

Mr. PECK. Actually, I think just the Capitol, the White House. I don't know if State Department.

Ms. NORTON. Mr. Porcari, do you have to do the trucks on your own?

Mr. PORCARI. Yes, we do. Our loading dock facility has, for example, x-ray facilities for packages coming in. It has bollards.

Ms. NORTON. See what I mean. You know what a waste that is. Whereas the Ronald Reagan building has, I hate to say this, a higher level security in my view. They figured it out. 20 minutes, if you are not there in 20 minutes bye bye, you don't get in. But there is a central facility for doing it. Mr. Porcari, and probably we did this, or at least the facility, it was possible to do it when we created the building. So if there is no central facility then they are not going to be caught with trucks coming in that had not gone through the right security. So I would bet you that every agency is somehow trying to screen these trucks. This goes to what Mr. Dowd said about some central place.

Mr. PECK. If what you are saying is we have not shared best practices across our buildings in Washington, I think you are absolutely right.

Ms. NORTON. Well, what does the ISC do if they don't do that?

Mr. PECK. Well, you know, I don't know enough to say. I think they have been looking at kind of high level security criteria and the more fine grained security practices that are really important

are—have somewhat been left to be customized agency by agency and building by building.

Mr. GOLDSTEIN. For most of its history, Madam Chairman, the ISC has been an organization of really a one part time person. They have not really provided staff to that committee, so it has not always moved as quickly as might be hoped.

Ms. NORTON. Well, that is important to know. Where does that staff come from?

Mr. GOLDSTEIN. It comes from the Department of Homeland Security.

Ms. NORTON. Mr. Schenkel, on page 5 I noted in your testimony you say you took steps immediately after the GAO report was issued in early July. This has to do with the bomb making materials, et cetera. How do you track implementation and progress of the steps you have taken? Understand that GAO didn't go to one or two buildings. They went and not just in one city, and that is why it was disturbing.

Mr. SCHENKEL. Yes, ma'am. It was very disconcerting and as soon as Mr. Goldstein and his team came and briefed us we took immediate steps. We formed a tiger team and started doing a gap analysis in regard to what things had to be covered.

Ms. NORTON. Well, let's start with the magnetometer. It looked like even the training at the magnetometer basis, for example, liquids coming into Federal buildings, I don't know if the magnetometers can capture that or what you can do about that.

Mr. SCHENKEL. Well, we did do a blanket purchase agreement on new x-ray machines that will differentiate between water and then more viscous liquids.

Ms. NORTON. Very important.

Mr. SCHENKEL. Yes, ma'am.

Ms. NORTON. Between water and other liquids.

Mr. SCHENKEL. Yes, ma'am. Yes, ma'am. In addition—

Ms. NORTON. What have you done to assure that the FPS guards and contract guards are properly trained since part of this had to do with people and their training at the magnetometer?

Mr. SCHENKEL. Yes, ma'am. There are several things that we have done. We initially issued an immediate training bulletin that provided information to each individual security guard as to—

Ms. NORTON. What good is that? Don't they need some retraining?

Mr. SCHENKEL. Yes, ma'am. I am getting to that. Yes, ma'am. In addition to that, part of the tiger team in addition to the actual bulletin we also produced a training video that every one of the single guards had to go through. In addition to that we have also retrained cadres of inspectors that are in process right now of actually doing hands-on training to all of our contract security guards. Also, when we conduct our operation shields or our guard post inspections. If we find discrepancies we make remedial training an urgent mission right on the spot. We don't wait or report it later on. We take immediate action and retrain the guards.

As part of the tiger team's review we have determined that yes, we do need to be much more involved and more actively involved in the training of the contract security guards. We are in the proc-

ess now of actually determining the appropriate numbers of inspectors and trainers that would be necessary to enact that.

Ms. NORTON. Well, some of this is quite reassuring. And I thank you, Mr. Schenkel. I know, not only on behalf of the Committee, but on behalf of people in these unknown buildings. For security reasons we of course will not name the buildings. And we know you will take these reports seriously.

Let me ask you, Mr. Schenkel, and for that matter Mr. Peck, Mr. Goldstein, I experienced the shock of 9/11. And believe me, we went through trial and error. I am also on the Aviation Subcommittee, so I think I have just seen it all in terms of us stabbing at what we can do, trying it out, not often enough, pulling it back, seeing wonderful cooperation on both sides of the aisle, trying to keep the country open.

One thing that we did after 9/11 was to federalize the security at airports. Before that it was much like what I hear the Federal buildings are doing, you know everybody try to do it the best you can. There is some overall guidance. You can believe the airports had some overall guidance. But in our judgment, security was important enough to at least have some uniformity. And that uniformity goes across the board. It fits Washington, D.C. And it fits far smaller cities, medium size cities. Yes, it is tailored and particularized, but this is a model for the United States of America. And all I can say is we haven't been struck again and it is had a deterrent effect we think at least.

Why can't FPS set up a model that is similar to the TSA model which standardizes certain elements of security even given the vast differences between a New York, a Washington, D.C., for that matter, and I don't know, a Nashville, Tennessee and a Podunk, call its name out. If we can do that across this vast Nation, why isn't there a standard model and then we work up from there or down from there?

Mr. SCHENKEL. Ma'am, that has been the effort of FPS over the last several years.

Ms. NORTON. But you heard testimony here that shows that that is not the case.

Mr. SCHENKEL. Yes, ma'am.

Ms. NORTON. There is the Ronald Reagan Building and then there is the DOT.

Mr. SCHENKEL. I think the Ronald Reagan Building probably represents the optimum of what we are all trying to get. Mr. Peck and I have already entered in discussions since just his recent arrival and prior to that his predecessors and his security office and FPS have been working on minimal security standards. Inconsistency is one of the most challenging things when it comes to security. Inconsistency.

Ms. NORTON. You have been working on minimal—

Mr. SCHENKEL. Security standards.

Ms. NORTON. Since when and when will they be out?

Mr. SCHENKEL. We have no idea when they will be out because we don't know that we can enact them. Currently there are not the authorities.

Ms. NORTON. You have no idea when they will be out because, say that again?

Mr. SCHENKEL. I have no idea when they will be out because we don't have the authorities to actually—

Ms. NORTON. So you are doing what you don't have the authority to do. Who has the authority?

Mr. SCHENKEL. At some point the ISC would have the authority to publish that. But what we are trying to determine is a minimal standard that would be consistent—

Ms. NORTON. I am not asking you to tell me when Secretary Napolitano will sign off on something. I am asking you when you will be ready. I am asking you within your power. You can't speak to maybe ICE. I will speak to ICE especially on my Homeland Security Committee. You have got the agency that is under scrutiny here. So if you have been working, I need to know when you think you will be ready with a minimal security model that we can begin to work from in the Congress.

Mr. SCHENKEL. Ma'am, I really couldn't answer that because there is a couple of other things—

Ms. NORTON. Well, let me tell you what, Mr. Schenkel. You are going to within 30 days provide this Committee with information on your goal for getting a plan, doesn't have to get done, getting a plan to ICE so that we can then hold those accountable beyond you. You alone are accountable because—not ICE, but you have the authority to look at the agency under your control. I am not asking you when you are going to get it done. I am asking you, I am telling you this much. If it is open ended it is going to get done whenever you get ready. I am also telling you that this is a matter of security. And therefore, I need to know when you intend to have a plan. Do you intend to have a plan within 5 years, do you intend to have a plan within 5 months? Do you intend to have a plan within 5 weeks? I only know how to work in a system by goals and timetables. 30 days. That is all you have to get to us.

I want to ask Mr. Moses a question. You have within your jurisdiction the quintessential model, you have just heard others say that they would like to see that model looked at more closely for possible application elsewhere. You have also heard that the DOT is operated under a model which puts everybody virtually, except its employees, off limits. Yet the Ronald Reagan welcomes a million people. And you are responsible for security in this region.

Would you favor a model that is more standardized based on what apparently has been worked out at the Ronald Reagan Building?

Mr. MOSES. Chairwoman, inconsistent with the Director—

Ms. NORTON. I understand by the way your boss is sitting there. I am asking you, since you are the one that has been closest to the model, you don't know whether Mr. Schenkel is going to be able to use it or not. But he is going to look to you to say is this something you think has utility outside of this one building in the United States or not?

Mr. MOSES. Yes, ma'am. As the previous witness mentioned on the earlier panel, that requires close coordination and certainly, within the National Capital Region of the Federal Protective Service we are willing to work with the Department of Transportation to ensure, as you mentioned with the Deputy Secretary, that we

are willing to consult with them to ensure that we can have the same application that we have in the Ronald Reagan Building.

Ms. NORTON. Now you know there may be flaws in this model. The reason I keep holding it up is normally when we find models for the Federal sector they are outside of the Federal sector. We were delighted that the Federal sector had created, without any model of its own, what appeared to be a security within security, you know, we usually ask for just security one by one. And here we looked and found the most complicated security had been worked out fairly well, it seemed to us, in this one building. And we thought, wow, wouldn't we want to grab on that model. And we even thought that some of our colleagues in the private sector with whom we work so closely would be interested in the model. That is why I want to know more about the model and I would like the NCPC to look at the model in that light whereby you almost look like you have got a test case, like somebody said, and they didn't, let's test it to see whether or not within the same facility we can look at one facility as a control group, almost, and another one and let's see how it comes out. Without meaning to do so, it looks like you have done it. Mr. Dowd?

Mr. DOWD. Yes, Madam Chairman. What I think this points out from NCPC's perspective is the important of balancing security with other values. And what I think the Ronald Reagan Building points out to us is that if we create a value of access to that building then we can work with the security and make sure we accomplish both. Just like we do on some of the physical security projects. Around the Washington Monument, for example, the initial proposals were for a ring of bollards around the monument. And our commission said no, that is not acceptable. We value this space too much to let that security intrude upon it. And so we worked hard and ended up with a security solution that is just as secure, but yet we retain those other values that are important to us.

So I think that is kind of the common thread that I see in these challenges, that we have to make sure we respect those other values that are important to us.

Ms. NORTON. Well, what you have said is very important. I would phrase it this way. I believe that everybody working on security has done what he has supposed to deal with security. They have been given only one mission. What you call a value, I call a mission. Mr. Moses has two missions. Mr. Moses, I know how to keep everything secure. Just shut all y'all out of it. So keeping buildings secure is not rocket science. The great American innovative spirit could come out in glorious ways if, in fact, agencies regarded their mission as two-sided; that security without openness is unacceptable, openness without security is unacceptable. Here you don't see me quantifying the two because I don't know how to do that. All I know is that initially in the Capitol, this was a terrible place afterwards, and even though sometimes there are long lines, I don't complain a lot about the Capitol. We are always looking at it. We have complaints about the Capitol Visitor Center, based on experience.

Mr. Porcari's point that, you know, it is not static. My only correction is that it has been, for the most part. We haven't heard of

changes that have occurred. We have heard of some regulations that may make changes occur. We didn't know when they were going to be issued. It hasn't been a continuing review, because frankly it hasn't been anybody's business. There has been this large group, the ISC, which means that all of them are responsible so nobody's responsible. We are going to see to it that somebody is responsible and accountable, and that the mission is a two-sided mission.

Before I let you go, there has been a big concern about something that otherwise I regard as a very important part of what security in every building should be. After we get some kind matrix about how to keep a building secure, then go to the next set about how to keep this building in particular secure, we would not begin to have put together what was needed until we had done the vital consultation with those who go to work every day in the building, and who, in some sense, knows it best. Well, our experience has been that they not only know it, at least from the point of view of going to work every day, they do it. These so called building security committees which have people from the agencies to sit on building security, they may be from, you know, the IT department, dealing with matters that have nothing to do with security. They may be from, somebody from the Secretary's office who is special assistant whose job really is to keep track of Members of Congress. But nevertheless, they sit together and we have been astounded at their influence.

What should be the role of the building security committees? Mr. PECK?

Mr. PECK. As I said before, I think the building security committees have been asked to perform a function that they should not have been asked to perform. They have been put in a position, whether overtly or it just grew that way, of making the decisions about security practices in a lot of buildings. And so, I mean, I have seen, I saw it before and this may have changed. But there were times when the Federal Protective Service and GSA together would say there is really a best practice that would allow you to have all the security you need in your building by doing this set of practices. And sometimes building security committees say but we were in another building and we saw them do something else so we would rather do it. And sometimes the other building they saw was a building with a different mission, a different level of security, a different level of needs. And so I believe that some of what you are talking about is—

Ms. NORTON. And GSA couldn't say, well, had no power to do anything about these civilians telling you that they want the same thing they have across the street.

Mr. PECK. Correct. And to be frank, the only way in which we have ever been able to say, we can't or won't do that is to say we don't have the resources to do it, and you don't have the resources to do it.

Ms. NORTON. Not only do we not have the resources to do it, but we work closely in conjunction with the Appropriations Committee. Nobody is going to have the resources to do it.

Mr. PECK. Correct.

Ms. NORTON. What we are doing here is the beginning of work that the Congress is going to do. If the agencies want to straighten it out themselves, that is the best way to do it. But we believe that the agencies are spending money because they can. After all, it is within their budget. They might spend it on something else. But we will be working with the Appropriation Committee as well. We would rather see you spend it on your mission. We believe that DOT does trucks because no central part of the Federal Government helped DOT to find a better way to do it and, therefore, they had no alternative.

So we are looking to work with all of you, not DOT nearly as much as with Mr. Peck. Mr. Peck, Mr. Goldstein, Mr. Dowd, Mr. Schenkel and Mr. Moses. Not so much the individual agencies, because we know that they have been left on their own to guard their own security and to take advice from their own employees. I don't believe—I am a small "d" democrat—believe in bottom up democracy. But I also am a Member of the Homeland Security Committee, and believe that at some point security trumps everything. After 9/11, security trumped everything as far as I was concerned until we figured out some way to make sure that we at least had a handle on not letting them come right back at us.

You will not see me among the Members of Congress advising the President that we ought to get out of Afghanistan right away. You will not see me saying that. I am sitting in the region that was struck. I hope none of my folks in New York are saying just walk away, Mr. President. You will see me telling him that there are some things to do besides start another Iraq, but you won't see me unmindful of the security concerns that each of you have raised. It would be only an authoritarian regime that would say once you have looked at what the agency wants, at its professional level, once you have looked at the template, go to it. That is not this country and that is not this Federal Government. It seems to me that the input of Federal employees is critical to the success of the homeland security mission.

Federal employees will be just like those who find today that there are new security alerts and so they have gone, television has gone out into the streets and saying, well, you know, what do you think that now that it is a little more inconvenient and it is interesting, almost across the board people are saying, look, we understand that they are trying after these arrests in New York to keep us all safe. After a while, people lose patience and they begin saying, well, why are they still doing this? Why are they still slowing up?

The building security people who talk to employees will be able to say to you what you would otherwise never know, that they have, in fact, seen people get through security with the guards talking to somebody instead of looking, or they don't know how somebody who appeared to need help and to be homeless got in the same elevator with them. How are you going to know unless the building security committee is alert? And how are you going to know things about the building? You can only know if you sit in that office and see ways that could be shored up without some of the ways that are being used now.

So I don't want to be heard to say that we want to professionalize everything any more than I am saying that what we have pointed out as issues for us can be laid at the table of anybody except the Congress of the United States. It is our oversight responsibility to bring these out and then to work with you. We bring them out. We are concerned and frustrated with them somehow but we do not stop with well, we have shown the world that this doesn't work. We use the hearing as a template to task staff to then go and help us help the agency find the way out that may have come forward from the hearings.

I am going to take this opportunity to thank you for spending so much time with us, understanding that you are educating us, helping us figure out what all of us are still trying to understand, and to thank you very much for your written testimony and for your willingness to sit with us as we ask you questions and learn from you and the experiences you have.

This hearing is adjourned.

[Whereupon, at 5:15 p.m., the Subcommittee was adjourned.]

**OPENING STATEMENT OF
THE HONORABLE RUSS CARNAHAN (M0-03)
HOUSE TRANSPORTATION AND INFRASTRUCTURE
ECONOMIC DEVELOPMENT, PUBLIC BUILDINGS, AND EMERGENCY
MANAGEMENT**

**Hearing on
Risk-based Security in Federal Buildings: Targeting Funds to Real Risks and
Eliminating Unnecessary Security Obstacles**

**Wednesday, September 23, 2009
2167 Rayburn House Office Building**


Thank you, Chairwoman Norton and Ranking Member Diaz-Balart for holding this hearing to examine existing security level categories in Federal buildings and the allocation of security funds.

I have grave concerns that a recently released Government Accountability Office (GAO) report revealed that the GAO was able to penetrate ten high security Federal buildings with liquid bomb making equipment and build actual bombs inside the facilities. Clearly there is inconsistency in the security standards applied to Federal buildings.

With the inventory of Federal buildings continuing to increase it is critical to ensure there is uniformity of security standards. I am especially concerned that the security of Federal buildings is often set of non-security personnel employed by tenant agencies through a Building Security Committee for each individual public building. As a result I believe it is difficult to gauge property risk in facilities and allocate Federal Protection Services resources properly.

In closing, I would like to thank our witnesses for joining us today and I look forward to their testimony.





STATEMENT OF
THE HONORABLE ELEANOR HOLMES NORTON
TRANSPORTATION AND INFRASTRUCTURE COMMITTEE
SUBCOMMITTEE ON ECONOMIC DEVELOPMENT, PUBLIC BUILDINGS AND EMERGENCY
MANAGEMENT
SEPTEMBER 23, 2009

**“Risk-based Security in Federal Buildings: Targeting Funds to Real Risks and
Eliminating Unnecessary Security Obstacles”**

Welcome to today’s hearing, especially our distinguished panels. I called this hearing as chair of this subcommittee and member of the Transportation and Infrastructure Committee. However, I also sit on the Homeland Security Committee and I represent the high-target nation’s capital. My committee work puts me in touch with the nation’s security needs at the highest levels. This work and our experience since the Oklahoma City bombing leave no doubt that the complexities of risk-based security in an open society continue to elude us.

Federal building security has little to do with risk-based threats today. The General Accounting Office was recently able to get bomb-making equipment past security at several federal buildings in the national capital region, where much of the new security has been focused. At the same time, tax-paying citizens are unable to enter some buildings to use the restrooms or restaurant facilities. The security in federal buildings is not uniform when it should be and, sadly, not professional or even appropriately in the hands of the Department of Homeland Security and the Federal Protective Service. Non-security personnel control much of the security for many agencies.

I introduced HR 3555, the United States Commission on an Open Society with Security Act on the eighth anniversary of 9/11, as an increasing variety of security measures have proliferated throughout the country without any expert or uniform guidance on evaluating risks to security and without much thought about the effect on common freedoms and citizen access.

Federal facilities, where millions of federal employees work and citizens come for service, have been the chosen targets for major terrorist attacks on our country. After the

attacks on the Pentagon and the Alfred P. Murrah Oklahoma City federal building, terrorists have left no doubt that federal facilities, as symbols of the United States government, are targets. Consequently, this documented pattern of terrorist assaults on federal assets and consistent threats since 9/11 have required continuing high levels of vigilance to protect both federal employees and the visitors who all use federal facilities.

When the Department of Homeland Security (DHS) was formed in 2002, the Federal Protective Service (FPS), charged with protecting federal sites, was transferred from the General Services Administration (GSA) to the newly created DHS and placed within Immigration and Customs Enforcement (ICE). Although the Committee supported the transfer, we insisted that FPS officers and guards be used exclusively by the FPS to continue the necessary protection of federal sites. However, starting in February 2005, the Chairman and I have had to send a series of letters to DHS, and this subcommittee has held hearings questioning the placement of FPS within the ICE, inappropriate use of funds, and a major shift from protection to inspection. These concerns have strong bipartisan support, with both Chairman Oberstar and Ranking Member Mica both expressing their own views about the gravity of the FPS situation.

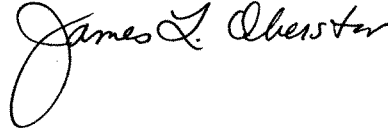
Now comes a GAO report to confirm that the FPS, the nation's first federal police force, established in 1790, and its contract guard force, have been rocked by inadequate funding, staffing and training that cast doubt on its ability to carry out its core missions to protect facilities, to complete building security assessments in a timely and professional manner, and to monitor and oversee contract guards. GAO reports, ominously, that proactive patrols have been eliminated at many GSA facilities, in spite of the fact that "multiple governmental entities acknowledge the importance of proactive patrol in detecting and preventing criminal incidents and terrorism-related activities."

Given these radical changes at FPS, at odds with its statutory mandate, who can be surprised that today the GAO will testify today concerning how GAO testers were able to get bomb-making equipment past security at several federal buildings? At the same time, tax payers are unable to enter some federal buildings without escorts or other obstacles to the access to which they are entitled. Surely, we are smart enough to keep terrorists out without making it virtually impossible for U.S. taxpaying citizens to get into federal buildings. Risk based security will be impossible as long as the requirements are set by a hodge-podge group, who can choose their own security requirements, without regard to evaluated risks and the big picture security concerns of each region. What passes for federal security lacks the needed consistency, rationality and accountability outside the particular agency. Non-security personnel are setting the agenda and calling the shots building by building. We can do better, but only if we recognize and then come to grips with the complexities associated with maintaining a society of free and open access in a world characterized by unprecedented terrorism. Following the terrorist attack on our country on 9/11, all expected additional and increased security adequate to protect citizens against this frightening threat. However, the American people also expect government to undertake this awesome new responsibility without depriving them of their personal liberty. The place to begin is with a high-level presidential commission of experts from a broad spectrum of relevant disciplines – not military and security experts

alone - who can help chart the new course that will be required to protect our people and our precious democratic institutions and traditions at the same time. When we have faced unprecedented and perplexing issues in the past, we have had the good sense to investigate them deeply in order to resolve them. Examples include the National Commission on Terrorist Attacks Upon the United States (also known as the 9/11 Commission), and the Kerner Commission that investigated the uprisings that swept American cities in the 1960s and 1970s. The important difference in my bill is that the Commission would seek to act *before* a crisis-level erosion of basic freedoms takes hold and becomes entrenched. Because global terrorism is likely to be long lasting, we cannot afford to allow the proliferation of security that does not require and is not subject to expert oversight or analysis of technological advances and other alternatives that can do the security job as well and without the severe repercussions on freedom and commerce.

Following today's hearing I intend to move H.R. 3555 to help us find the necessary balance by establishing a presidential commission of experts from a broad spectrum of disciplines to investigate how to maintain democratic traditions of openness and access while responding adequately to continuing substantial security threats posed by global terrorism. The need for a high level commission is imperative to look at issues, from makeshift security and make-work checkpoints that are posted in the streets, even when there were no alerts, to the use of off-the-shelf technology used without regard to effects on privacy and openness.

We are open to all suggestions and recommendations concerning the still developing work of keeping us safe and open. We have confidence that our people and those in federal agencies can do both. We will listen carefully to how these agency officials plan to balance keeping citizens safe in an open society. I intend to move this bill following today's hearing. We welcome all the witnesses. Each of you is essential to this hearing. We appreciate your time and effort in preparing testimony.



STATEMENT OF
THE HONORABLE JAMES L. OBERSTAR
CHAIRMAN, COMMITTEE ON TRANSPORTATION AND INFRASTRUCTURE
SEPTEMBER 23, 2009
“Risk-based Security in Federal Buildings: Targeting Funds to Real Risks and
Eliminating Unnecessary Security Obstacles”

Good morning. I would like to thank Chairwoman Norton for her vigilant oversight of the Federal Protective Service and security in federal buildings. Since FPS was moved to the Department of Homeland Security (DHS) in 2002, and its placement within the Immigration and Customs Enforcement (ICE) division I remained concerned about its ability to provide security in and around federal buildings. Along with Chair Norton I strongly support the transfer the Federal Protective Service to the National Protection and Program Directorate within DHS.

The Committee is fully aware FPS has experienced problems with managing the guard service and has been stymied in setting up uniform security standards across country. Since we take our stewardship of this great organization very seriously we are especially concerned about the recent GAO report regarding security breaches in federal buildings.

This recent GAO report documented a GAO “security penetration” exercise. The GAO, using a specialized team of its own security experts, penetrated security in 10 buildings in 3 cities. During the exercise the team entered 10 buildings with bomb making materials and assembled in restrooms and put together a “false bomb”. The team entered the buildings, assembled, moved about these federal buildings, and entered Congressional offices undetected by building security.

These are disturbing findings but we have been briefed and know that FPS is struggling to correct the many deficiencies in its contract guard program, and to develop a building entrance policy that meets the demands of public access while also providing adequate security.

I agree with the Chair of this Subcommittee that it is distressing that the federal government has spent hundreds of millions on security for federal buildings and, as the GAO has pointed out, that federal buildings have significant gaps in security. Bluntly said, we are not getting what we are paying for. I look forward to hearing from our witnesses today as we discuss how to assist FPS in making federal buildings secure. I would also like to thank the Department of Transportation Deputy Secretary John Porcari for testifying today. I look forward to working with you on this issue and many others.

**Testimony of William G. Dowd
Director, Physical Planning Division,
401 – 9th Street, NW, Suite 500, Washington, D.C. 20004
National Capital Planning Commission
(202) 482-7200
Subcommittee on Economic Development, Public Buildings,
and Emergency Management Oversight Hearing
September 23, 2009**

Good afternoon, Chairwoman Norton, and Members of the Subcommittee. My name is Bill Dowd, and I am the Director of the Physical Planning Division of the National Capital Planning Commission, also known as NCPC within the National Capital Region. The National Capital Planning Commission is the federal government's central planning agency for the nation's capital and includes representatives from the Department of the Interior, Department of Defense, General Services Administration, the Mayor of the District of Columbia, the Council of the District of Columbia, the United States House and Senate Committees with oversight responsibilities in the District of Columbia, and individuals appointed by the President of the United States and the Mayor of the District of Columbia.

I am very pleased to have this opportunity to speak with you today about NCPC's role in trying to balance legitimate needs for physical security with undesirable impacts to important public spaces in our nation's capital. Unlike other cities across the country, as the seat of our federal government, Washington D.C. has a significant concentration of federal office buildings, museums, and national icons that warrant some level of protection. The most typical and visible form of physical security in our city is vehicle barriers (planters, jersey barriers, and bollards) located in our treasured public spaces. These public spaces, including sidewalks and building yards, accommodate a vast range of uses, and provide for mobility and enjoyment by the public. However, barriers sometimes detract from the sense of openness that is so important to our capital city.

In the National Capital Region, NCPC is responsible for the oversight of all physical development proposals on federal land. It is through this capacity that NCPC has developed extensive first-hand experience with the challenges of providing physical security in a city known around the world for its distinct public spaces. Our Commission understands that access to our government, as well as the important public spaces that define our nation's capital, is worthy of our protection.

NCPC is concerned about the continuing challenges of balancing security and accessibility. Over the past decade we have worked hard to minimize the impacts that physical security measures have on the public spaces that define the city and represent our democratic values.

- In response to the unsightly security features erected in Washington D.C. after the tragic 1995 bombing to a federal building in Oklahoma City, NCPC prepared and adopted *Designing for Security in the Nation's Capital*. Released in November 2001 this report identified an approach to designing future security features in Washington that would reduce their impact on public spaces;
- Following 9/11, NCPC published the *National Capital Urban Design and Security Plan* in October 2002. This plan provided specific guidance for the design of contextually sensitive physical security features appropriate for use in the monumental core of the city;
- In our review capacity, NCPC has regularly worked with applicant agencies over the past ten years to reduce the impacts of proposed security improvements on the environment and public space. For example, NCPC was instrumental in guiding development of the landscaped security solution on the Washington Monument grounds that is widely praised as a successful marriage between landscaped amenities and improved security;
- NCPC also initiated efforts to improve the urban design and security of *Pennsylvania Avenue in Front of the White House* and helped ensure that this important project was completed prior to the 2005 Presidential inauguration;
- In 2006, NCPC published a booklet on *Designing and Testing of Perimeter Security Elements* to share technical information about the design of crashworthy barriers; and most recently
- In 2008, NCPC assembled a Security Task Force to address the impacts that security projects were continuing to have, both individually and cumulatively, on the city's important public spaces. The Task Force included members of NCPC, but also included participation from other government security professionals including the Department of Homeland Security and the United States Secret Service.

Through this one-year effort, NCPC's Security Task Force reached several conclusions regarding the challenges of physical security. It also developed alternatives to better balance the need for security with the value of providing and maintaining openness in the nation's capital. The Security Task Force found that:

- Because the probability of any specific type of attack on a facility is so difficult to quantify, the current determination of risk is based primarily on the vulnerability of a facility and the potential consequences of an attack. This approach to assessing risk often leads to proposals for extremely robust security solutions;
- Existing security standards may seem appropriate in cities with only a few facilities that need protection but these standards, which are focused on increasing protection and physical stand-off at individual facilities, are more challenging in cities with many assets such as Washington D.C.;

- Because individual federal agencies are responsible for securing only their individual facilities, area-wide security improvements that could benefit the entire city or monumental core, are less likely to be identified and implemented. For example, one component of London's layered approach to security is their "Ring of Steel" that improves security within an entire district through the use of strategically placed guard stations and closed circuit television cameras with license plate recognition capabilities; and
- Security proposals for individual buildings are often developed specifically to satisfy existing security standards, not balancing improved security against other public, or environmental, impacts.

NCPC's Security Task Force determined that bringing together the views of planners, designers, security professionals, federal landholding agencies; and federal and local oversight agencies to guide the planning and development of future security improvements can help meet these challenges. These groups need to work together to:

- Prioritize security improvements at federal facilities;
- Identify the most cost-efficient way to address our most critical security needs;
- Coordinate future security improvements to make sure that they address and respect the needs of federal and local facilities in the city; and
- Ensure that individual and cumulative impacts to public space, public access, and the environment are fully considered before implementing physical security projects in the future.

While it is important to make sure that we protect our nation's most valuable assets, we must do so in a way that considers the impacts of our actions, and which does not unduly harm the public spaces, or the public access to our government.

Thank you for inviting me to share NCPC's perspective on the challenging work to balance the need for improved physical security with the potential impacts that physical security projects have on public spaces and access to our government facilities.

Question for the Record
Response to the
Subcommittee on Economic Development,
Public Buildings, and Emergency Management Oversight
November 18, 2009

On September 23, 2009, the National Capital Planning Commission provided testimony before the Subcommittee on Economic Development, Public Buildings, and Emergency Management Oversight on the subject of Risk-Based Security in Federal Buildings. The National Capital Planning Commission offers the following response to the Question for the Record received on October 21, 2009.

Question

On page 3 of your testimony you mention the need to prioritize security improvements at federal facilities. How would NCPC prioritize such improvements?

Response

The National Capital Planning Commission reconvened the agency's Security Task Force to address concerns related to this issue in January 2008. The Task Force included Commission representatives from the Department of Defense, the Department of Interior, the General Services Administration, the US Senate Committee on Homeland Security and Governmental Affairs, the US House of Representatives Committee on Oversight and Government Reform, the Council of the District of Columbia, and the Mayor of the District of Columbia. In addition, work of the Task Force was informed by Task Force Associate Members that represented the General Services Administration's Public Buildings Service, the Architect of the Capitol, the Department of Homeland Security's Office of National Capital Region Coordination, the Interagency Security Committee, and the US Secret Service. This Task Force concluded that physical security improvements in the nation's capital should be better coordinated and prioritized, and that in order to accomplish this goal, there are two major actions that need to take place. The first action would be to prioritize physical security requirements at federal facilities throughout the city; and the second action would be to identify the most efficient security solutions that satisfy those needs and have the least impact on our open society.

Today, security assessments that identify physical security requirements in the nation's capital are prepared by agencies for individual facilities. Having these assessments done by different groups, with different perspectives, results in a list of security needs that does not necessarily address the relative value of each individual security improvement. To more accurately understand and prioritize the city's physical security needs, a single group or agency should conduct security risk assessments throughout the city to allow the needs to actually be prioritized.

Once the physical security needs have been prioritized, the next action would be to identify and prioritize a range of security solutions. In order to ensure that scarce resources are used most effectively, a broad range of security solutions should be considered. These solutions would include improvements at individual facilities, but must also include initiatives designed to improve security for all facilities in a larger geographical area. Examples of such comprehensive solutions could include district-wide efforts to manage freight and truck traffic; as well as coordinated security solutions for individual facilities that are located in clusters.

Developing a prioritized plan of physical security requirements in the nation's capital should be prepared by a diverse group that understands the science of security threats and risks; is able to coordinate security decisions for a broad range of assets; and is able to balance the value of enhanced security with the impacts to our public spaces and other valuable public resources.

Without a comprehensive and coordinated approach to federal security within the District of Columbia, security will continue to be implemented through a building-by-building approach. This current approach neither identifies our facilities that are most in need of enhanced security, nor does it adequately consider the cost effectiveness of more comprehensive solutions that may be less intrusive and more effective.

**Subcommittee on Economic Development, Public Buildings and
Emergency Management**

**“Risk Based Security in Federal Buildings: Targeting Funds to Real
Risks and Eliminating Unnecessary Security Obstacles.”**

September 23, 2009

Prepared Testimony of John E. Drew

Chairman of Trade Center Management Associates

Ronald Reagan Building and International Trade Center

1300 Pennsylvania Avenue, NW

Washington, D.C 20004

Phone: 202.312.1300

Good Afternoon Madam Chair:

My name is John E. Drew, and I am the Chairman of Trade Center Management Associates, or

TCMA. We appreciate being given the opportunity to appear here today. Thank you very

much. I have prepared some brief remarks if I may summarize them at this time?

TCMA has had the privilege of being the operator of the public portion of the Ronald Reagan

Building and International Trade Center since the building officially opened in 1998. We work

for the U.S. General Services Administration, the owner of the building. After the Pentagon we are the largest Federal building at 3.1 million square feet and the largest in Washington, D.C. No one knows better than you Madam Chair that the Reagan Building was created with a unique Congressional mandate to function as a mixed use building with a trade promotion program that we organize, that creates and enhances opportunities for American trade and commerce and that supports the Federal agencies who are involved in trade.

TCMA's responsibility is to support the GSA in their implementation of this Congressional mandate and our responsibility is limited to the "International Trade Center" which consists of the public spaces inside and outside of the Ronald Reagan Building and is kind of a "building within a building". Our team operates the International Trade Center with a diverse and passionate workforce of over 550 full and part time members (including two unions). We are proud to say that we are Washington's busiest conference and special events location. We produce and provide a full range of services to over one thousand meetings and events a year and we welcome an estimated 1,000,000 visitors. Our meetings and events are diverse and range from the recent US/China Economic Recovery Summit that President Obama, and Secretary Clinton and Treasury Secretary Geithner organized in July, to a wedding taking place

this weekend organized by US Weekly Magazine and the weddingchannel.com. The groom is a former soldier stationed in Iraq. In addition, we operate Washington D.C.'s largest parking garage that accommodates nearly 2,000 vehicles. This includes hundreds of cars each day that are visiting the Reagan Building for conference, attending meetings at Federal agencies, or who are touring the city. We produce a number of activation projects that help the building fulfill its mission of connecting the central business district with the National Mall. In particular we host LIVE! On the Woodrow Wilson Plaza, which is a free summertime concert series enjoyed this year by over 75,000 people. It is also worth mentioning that in order to fulfill the mission of the building to foster trade we have a group specifically devoted to organizing and bringing in upwards of 150 trade related events to the building each year.

We have a diverse tenant mix in the building. Our public food court with more than twenty vendors serves as the cafeteria for the Federal workforce in the building. It also hosts hundreds of thousands of visitors; many of them school children, who are on organized tours of Washington. The building is home to government agencies such as EPA, US Customs and Border Protection and USAID. In addition, our tenants located throughout the building and in our office tower include private sector global organizations, the University of Maryland's Robert

Smith School of Business, international affairs offices of multinational corporations, foreign entities not for profit organizations, and international trade consultants.

My testimony this afternoon is focused on building security and how it is created and sustained.

My remarks are limited to the security environment for the public spaces only, the International Trade Center. This security is provided by the Department of Homeland Security through the Federal Protective Service using Federal Police Officers and an armed contract guard force.

During normal business hours, the Reagan Building has perimeter security at six different street entrances including an entrance at the Federal Triangle Metro Station. These stations all include X-ray and Magnetometers and everyone is required to present a picture ID to a uniformed guard. Some entrances are open around the clock. In addition, all vehicles entering the Reagan Building garage are screened using, I think the euphemistic phrase is, "technical means" for explosive devices. In addition all trunks and cargo spaces are inspected visually by the guards.

We also get a large number of daily truck and van deliveries to our food court, restaurants, and catering kitchens and to support the events at the conference center. Many trucks also enter to support the Federal tenants. One hundred percent of these larger vehicles are scanned using a drive-through X-ray machine off site a few blocks away from the Reagan Building operated by FPS. All of the drivers have to have been pre-cleared, produce proper ID and then the vehicles are sealed and then re-inspected when they arrive at the Reagan Building before they go to our loading docks downstairs. Over 20,000 trucks a year were inspected in 2008 through the remote screening location.

Finally, in addition to these human and technical security barriers, we also have canine officers present on site for random checks and to respond to any issues that might arise. And, as I said, this is just the security apparatus for the public spaces. The Federal office towers have their own separate security stations and procedures inside the Building.

Turning back to the public spaces in the International Trade Center, the security was increased after 9/11 and perimeter security was installed. Until then, all 50 some doors to the public

spaces were open to the public with no perimeter security. After 9/11 the measures I have described above were implemented. Initially, we feared that this comprehensive perimeter screening would prove an impediment to our conference center guests and tourist visitors. But, as it turned out everyone understood the heightened risk and now, I believe, actually consider the perimeter security to be a positive aspect for the Reagan Building.

Of course, this generally positive view of it is made possible only because of the significant resources and coordination committed by GSA and FPS to make this happen. We have terrific working level cooperation and a mutual understanding that "security comes first, but the business of Government and the Reagan Building has to continue" and that the building must be open to the public. We have held over 10,000 events with literally millions of visitors and a wonderful institutional knowledge has been developed that allows everyone to work and function together. The working partnership at the Reagan Building between Homeland Security and GSA grows stronger all the time. We have established protocols for visits by the President of the United States, working also with Secret Service who has a Reagan Building coordinator. We are also ready for weekly visits by foreign dignitaries to both the Federal space and the International Trade which is coordinated with the Bureau of Diplomatic Security. The Reagan Building also services busloads of school children who daily come to the food court and to see

the piece of the Berlin Wall we have on display. Every one of the visitors is security screened through an airport style X-ray machine and all packages; backpacks, etc are put through a magnetometer.

This kind of seamless and layered security would not exist without close coordination, communication and cooperation. There are regular weekly and monthly meetings with the Federal tenants and the Reagan Building security staff to meet and talk about security issues and follow through on any updated procedures and issues. Members of our staff take part in weekly security meetings with the building security staff to describe all upcoming events and to coordinate event related orders for additional guards, deliveries, and requests for K9 after hours screeners and coordinate VIP parking. This is to name but a few security related requests that might come up on a daily basis that all require constant communication and coordination.

In conclusion, I think that it is worth reiterating that all parties involved recognize that the safety of everyone who works at or visits the Reagan Building demands and deserves our daily attention. All parties involved seek practical solutions to maintain the level of security while

ensuring the safety of both the tenants and guests and pursuing the mission of the Ronald Reagan Building.

This concludes my prepared remarks Madam Chair, and I am pleased to answer any questions you and the committee may have.

Thank you very much.

United States Government Accountability Office

GAO

Testimony
Before the Subcommittee on Economic
Development, Public Buildings and
Emergency Management, Committee on
Transportation and Infrastructure

For Release on Delivery
Expected at 2:00 p.m. EDT
Wednesday, September 23, 2009

HOMELAND SECURITY

**Federal Protective Service
Has Taken Some Initial
Steps to Address Its
Challenges, but
Vulnerabilities Still Exist**

Statement of Mark L. Goldstein, Director
Physical Infrastructure Team



September 23, 2009

HOMELAND SECURITY

Federal Protective Service Has Taken Some Initial Steps to Address Its Challenges, but Vulnerabilities Still Exist


Highlights

Highlights of GAO-09-1047T, a testimony to Subcommittee on Economic Development, Public Buildings and Emergency Management, House Committee on Transportation and Infrastructure

Why GAO Did This Study

To accomplish its mission of protecting federal facilities, the Federal Protective Services (FPS), within the Department of Homeland Security (DHS), currently has a budget of about \$1 billion, about 1,200 full-time employees, and about 15,000 contract security guards.

This testimony is based on completed and ongoing work for this Subcommittee and discusses: (1) challenges FPS faces in protecting federal facilities and (2) how FPS's actions address these challenges. To perform this work, GAO visited FPS's 11 regions, analyzed FPS data, and interviewed FPS officials, guards, and contractors. GAO also conducted covert testing at 10 judgmentally selected level IV facilities in four cities. Because of the sensitivity of some of the information, GAO cannot identify the specific locations of incidents discussed. A level IV facility has over 450 employees and a high volume of public contact.

What GAO Recommends

GAO has ongoing work on FPS and plans to report its complete evaluation along with any recommendations at a later date.

View GAO-09-1047T or key components. For more information, contact Mark Goldstein at (202) 512-2634 or goldsteinm@gao.gov.

What GAO Found

FPS faces challenges that hamper its ability to protect government employees and members of the public who work in and visit federal facilities. First, as we reported in our June 2008 report, FPS does not have a risk management framework that links threats and vulnerabilities to resource requirements. Without such a framework, FPS has little assurance that its programs will be prioritized and resources will be allocated to address changing conditions. Second, as discussed in our July 2009 report, FPS lacks a strategic human capital plan to guide its current and future workforce planning efforts. FPS does not collect data on its workforce's knowledge, skills, and abilities and therefore cannot determine its optimal staffing levels or identify gaps in its workforce and determine how to fill these gaps. Third, as we testified at a July 2009 congressional hearing, FPS's ability to protect federal facilities is hampered by weaknesses in its contract security guard program. GAO found that many FPS guards do not have the training and certifications required to stand post at federal facilities in some regions. For example, in one region, FPS has not provided the required 8 hours of X-ray or magnetometer training to its 1,500 guards since 2004. GAO also found that FPS does not have a fully reliable system for monitoring and verifying whether guards have the training and certifications required to stand post at federal facilities. In addition, FPS has limited assurance that guards perform assigned responsibilities (post orders). Because guards were not properly trained and did not comply with post orders, GAO investigators with the components for an improvised explosive device concealed on their persons, passed undetected through access points controlled by FPS guards at 10 of 10 level IV facilities in four major cities where GAO conducted covert tests.

FPS has taken some actions to better protect federal facilities, but it is difficult to determine the extent to which these actions address these challenges because many of the actions are recent and have not been fully implemented. Furthermore, FPS has not fully implemented several recommendations that GAO has made over the last couple of years to address FPS's operational and funding challenges, despite the Department of Homeland Security's concurrence with the recommendations. In addition, most of FPS's actions focus on improving oversight of the contract guard program and do not address the need to develop a risk management framework or a human capital plan. To enhance oversight of its contract guard program FPS is requiring its regions to conduct more guard inspections at level IV facilities and provide more x-ray and magnetometer training to inspectors and guards. However, several factors make these actions difficult to implement and sustain. For example, FPS does not have a reliable system to track whether its 11 regions are completing these new requirements. Thus, FPS cannot say with certainty that the requirements are being implemented. FPS is also developing a new information system to help it better protect federal facilities. However, FPS plans to transfer data from several of its legacy systems, which GAO found were not fully reliable or accurate, into the new system.

Madam Chair and Members of the Subcommittee:

We are pleased to be here to discuss the Federal Protective Service's (FPS) efforts to ensure the protection of the over 1 million government employees, as well as members of the public, who work in and visit the nation's 9,000 federal facilities each year.¹ There has not been a large-scale 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, Oklahoma. Nevertheless, the recent shooting death of a guard at the U.S. Holocaust Memorial Museum—though not a federal facility—demonstrates the continued vulnerability of public buildings to domestic terrorist attack. To accomplish its mission of protecting federal facilities, FPS currently has a budget² of about \$1 billion, about 1,200 full time employees, and about 15,000 contract security guards deployed at federal facilities across the country.

As the primary federal agency that is responsible for protecting and securing General Services Administration (GSA) facilities and federal employees and visitors across the country, FPS has the authority to enforce federal laws and regulations aimed at protecting federally owned and leased properties and the persons on such property. FPS conducts its mission by providing security services through two types of activities: (1) physical security activities—conducting threat assessments of facilities and recommending risk-based countermeasures aimed at preventing incidents at facilities—and (2) law enforcement activities—proactively patrolling facilities, responding to incidents, conducting criminal investigations, and exercising arrest authority.

¹For the purposes of this report, federal facilities are the 9,000 buildings under the control or custody of General Services Administration (GSA).

²Funding for FPS is provided through revenues and collections charged to building tenants in FPS-protected property. The revenues and collections are credited to FPS's appropriation and are available until expended for the protection of federally owned and leased buildings and for FPS operations.

This testimony is based on completed³ and ongoing work⁴ for this Subcommittee and discusses (1) challenges FPS faces in protecting federal facilities and (2) how FPS's actions address these challenges. To perform this work, we visited FPS's 11 regions, analyzed FPS data, and interviewed FPS officials, guards, and contractors. We also conducted covert testing at 10 judgmentally selected high risk facilities in four cities. Because of the sensitivity of some of the information in our report, we cannot specifically identify the locations of the incidents discussed. We conducted this performance audit from April 2007 to September 2009 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.

FPS Faces Several Challenges That Hamper Its Ability to Protect Federal Facilities

FPS faces a number of challenges that hamper its ability to protect government employees and the public in federal facilities. For example, these challenges include (1) developing a risk management framework, (2) developing a human capital plan, and (3) better oversight of its contract security guard program.

FPS Has Not Implemented a Risk Management Framework for Identifying Security Requirements and Allocating Resources

In our June 2008 report we found that in protecting federal facilities, FPS does not use a risk management approach that links threats and vulnerabilities to resource requirements. We have stated that without a risk management approach that identifies threats and vulnerabilities and the resources required to achieve FPS's security goals, there is little assurance that programs will be prioritized and resources will be allocated to address existing and potential security threats in an efficient and

³GAO, *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), 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), and GAO, *Homeland Security: The Federal Protective Service Faces Several Challenges That Hamper Its Ability to Protect Federal Facilities*, GAO-08-683 (Washington, D.C.: June 11, 2008).

⁴We plan to provide Congress with our complete evaluation at a later date.

effective manner. While FPS has conducted risk related activities such as building security assessments (BSAs), we have reported several concerns with the Facilities Security Risk Management system FPS currently uses to conduct these assessments. First, it does not allow FPS to compare risks from building to building so that security improvements to buildings can be prioritized across GSA's portfolio. Second, current risk assessments need to be categorized more precisely. According to FPS, too many BSAs are categorized as high or low risk, which does not allow for a refined prioritization of security improvements. Third, the system does not allow for tracking the implementation status of security recommendations based on assessments.

BSAs are the core component of FPS's physical security mission. However, ensuring the quality and timeliness of them is an area in which FPS continues to face challenges. Many law enforcement security officers (LESOs)⁵ in the regions we visited stated that they do not have enough time to complete BSAs. For example, while FPS officials have stated that BSAs for level IV facilities⁶ should take between 2 to 4 weeks, several LESOs reported having only 1 or 2 days to complete assessments for their buildings, in part, because of pressure from supervisors to complete BSAs as quickly as possible. Some regional supervisors have also found problems with the accuracy of BSAs. One regional supervisor reported that an inspector was repeatedly counseled and required to redo BSAs when supervisors found he was copying and pasting from previous assessments. Similarly, one regional supervisor stated that in the course of reviewing a BSA for an address he had personally visited, he realized that the inspector completing the BSA had not actually visited the site because the inspector referred to a large building when the actual site was a vacant plot of land owned by GSA.

⁵LESOs who are also referred to as inspectors are responsible for completing building security assessments and oversight of contract guards.

⁶The 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) 1995 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 which 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 federal 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 a Level V facility which include the White House and the Central Intelligence Agency. The Interagency Security Committee has recently promulgated new security level standards that will supersede the 1995 DOJ standards.

Moreover, some GSA and FPS officials have stated that LESOs lack the training and physical security expertise to prepare BSAs according to the standards. Currently, LESOs receive instructions on how to complete BSAs as part of a 4-week course at the Federal Law Enforcement Training Center's Physical Security Training Program. However, many LESOs and supervisors in the regions we visited stated that this training is insufficient and that refresher training is necessary to keep LESOs informed about emerging technology, but that this refresher training has not been provided in recent years. Regional GSA officials also stated that they believe the physical security training provided to LESOs is inadequate and that it has affected the quality of the BSAs they receive.

Further complicating FPS's ability to protect federal facilities is the building security committee structure. Building Security Committees (BSC) are composed of representatives from each tenant agency who generally are not security professionals but have responsibility for approving the countermeasures FPS recommends. However, in some of the facilities that we visited, security countermeasures were not implemented because BSC members could not agree on what countermeasures to implement or were unable to obtain funding from their agencies. For example, an FPS official in a major metropolitan city stated that over the last 4 years LESOs have recommended 24-hour contract guard coverage at one high-risk building located in a high crime area multiple times, but the BSC is not able to obtain approval from all its members.

In addition, FPS faces challenges in ensuring that its fee-based funding structure accounts for the varying levels of risk and types of services provided at federal facilities. FPS funds its operations through security fees charged to tenant agencies. However, FPS's basic security fee, which funds most of its operations, does not account for the risk faced by specific buildings, the level of service provided, or the cost of providing services, raising questions about equity.⁷ FPS charges federal agencies the same basic security fee regardless of the perceived threat to a particular building or agency. In fiscal year 2009, FPS is charging 66 cents per square foot for basic security. Although FPS categorizes buildings according to security levels⁸ based on its assessment of each building's risk and size,

⁷Some of the basic security services covered by this fee include law enforcement activities at GSA facilities, preliminary investigations, the capture and detention of suspects, and completion of BSAs.

⁸These levels range from I (lowest risk) to IV (highest risk).

this assessment does not affect the security fee FPS charges. For example, level I facilities typically face less risk because they are generally small storefront-type operations with a low level of public contact, such as a small post office or Social Security Administration office. However, these facilities are charged the same basic security fee of 66 cents per square foot as a level IV facility that has a high volume of public contact and may contain high-risk law enforcement and intelligence agencies and highly sensitive government records.

FPS's basic security rate has raised questions about equity because federal agencies are required to pay the fee regardless of the level of service FPS provides or the cost of providing the service. For instance, in some of the regions we visited, FPS officials described situations where staff are stationed hundreds of miles from buildings under its responsibility, with many of these buildings rarely receiving services from FPS staff and relying mostly on local law enforcement agencies for law enforcement services. However, FPS charges these tenant agencies the same basic security fees as buildings in major metropolitan areas where numerous FPS police officers and LESOs are stationed and are available to provide security services. Consequently, FPS's cost of providing services is not reflected in its basic security charges. We also have reported that basing government fees on the cost of providing a service promotes equity, especially when the cost of providing the service differs significantly among different users, as is the case with FPS. In our July 2008 report, we recommended that FPS improve FPS's use of the fee-based system by developing a method to accurately account for the cost of providing security services to tenant agencies and ensuring that its fee structure takes into consideration the varying levels of risk and service provided at GSA facilities. While DHS agreed with this recommendation, FPS has not fully implemented it.

FPS Does Not Have A Strategic Human Capital Plan to Guide Its Current and Future Workforce Planning Efforts

In our July 2009 report,⁹ we reported that FPS does not have a strategic human capital plan to guide its current and future workforce planning efforts. Our work has shown that a strategic human capital plan addresses two critical needs: It (1) aligns an organization's human capital program with its current and emerging mission and programmatic goals, and (2) develops long-term strategies for acquiring, developing, and retaining staff to achieve programmatic goals. In 2007, FPS took steps toward developing

⁹GAO-09-749.

a Workforce Transition Plan to reflect its decision to move to a LESO-based workforce and reduce its workforce to about 950 employees. However, in 2008, FPS discontinued this plan because the objective of the plan—to reduce FPS staff to 950 to meet the President's Fiscal Year 2008 Budget—was no longer relevant because of the congressional mandate in its Fiscal Year 2008 Consolidated Appropriations Act to increase its workforce to 1,200 employees.¹⁶ FPS subsequently identified steps it needed to take in response to the mandate. However, we found that these steps do not include developing strategies for determining agency staffing needs, identifying gaps in workforce critical skills and competencies, developing strategies for use of human capital flexibilities, or strategies for retention and succession planning.

Moreover, we found FPS's headquarters does not collect data on its workforce's knowledge, skills, and abilities. Consequently, FPS cannot determine what its optimal staffing levels should be or identify gaps in its workforce needs and determine how to modify its workforce planning strategies to fill these gaps. Effective workforce planning requires consistent agencywide data on the skills needed to achieve current and future programmatic goals and objectives. Without centralized or standardized data on its workforce, it is unclear how FPS can engage in short- and long-term strategic workforce planning. Finally, FPS's human capital challenges may be further exacerbated by a proposal in the President's 2010 budget to move FPS from Immigration and Custom Enforcement to the National Protection and Programs Directorate within DHS. If the move is approved, it is unclear which agency will perform the human capital function for FPS, or how the move will affect FPS's operational and workforce needs. We also recommended that FPS take steps to develop a strategic human capital plan to manage its current and future workforce needs. FPS concurred with our recommendation.

FPS's Ability to Protect Federal Facilities Is Hampered by Weaknesses in Its Contract Guard Program

FPS's contract guards are the most visible component of FPS's operations as well as the public's first contact with FPS when entering a federal facility. Moreover, FPS relies heavily on its guards and considers them to be the agency's "eyes and ears" while performing their duties. However, as we testified at a July 2009 congressional hearing, FPS does not fully ensure that its guards have the training and certifications required to be deployed to a federal facility. While FPS requires that all prospective guards complete approximately 128 hours of training, including 8 hours of x-ray

¹⁶Pub. L. No. 110-161, Division E, 121 Stat. 1844, 2051-2052 (2007).

and magnetometer training, FPS was not providing some of its guards with all of the required training in the six regions we visited. For example, in one region, FPS has not provided the required 8 hours of x-ray or magnetometer training to its 1,500 guards since 2004. X-ray and magnetometer training is important because the majority of the guards are primarily responsible for using this equipment to monitor and control access points at federal facilities. According to FPS officials, the 1,500 guards were not provided the required x-ray or magnetometer training because the region does not have employees who are qualified or have the time to conduct the training. Nonetheless, these guards continue to control access points at federal facilities in this region. In absence of the x-ray and magnetometer training, one contractor in the region said that they are relying on veteran guards who have experience operating these machines to provide some "on-the-job" training to new guards. Moreover, in the other five regions we visited where FPS is providing the x-ray and magnetometer training, some guards told us that they believe the training, which is computer based, is insufficient because it is not conducted on the actual equipment located at the federal facility.

Lapses and weaknesses in FPS's x-ray and magnetometer training have contributed to several incidents at federal facilities in which the guards were negligent in carrying out their responsibilities. For example, at a level IV federal facility in a major metropolitan area, an infant in a carrier was sent through the x-ray machine. Specifically, according to an FPS official in that region, a woman with her infant in a carrier attempted to enter the facility, which has child care services. While retrieving her identification, the woman placed the carrier on the x-ray machine.¹¹ Because the guard was not paying attention and the machine's safety features had been disabled,¹² the infant in the carrier was sent through the x-ray machine. x-ray machines are hazardous because of the potential radiation exposure. FPS investigated the incident and dismissed the guard. However, the guard subsequently sued FPS for not providing the required x-ray training. The guard won the suit because FPS could not produce any documentation to show that the guard had received the training, according to an FPS official. In addition, FPS officials from that region could not tell us whether the x-ray machine's safety features had been repaired.

¹¹X-ray machines are hazardous because of the potential radiation exposure. In contrast, magnetometers do not emit radiation and are used to detect metal.

¹²With this safety feature disabled, the x-ray machine's belt was operating continuously although the guard was not present.

Moreover, FPS's primary system—Contract Guard Employment Requirements Tracking System (CERTS)—for monitoring and verifying whether guards have the training and certifications required to stand post at federal facilities is not fully reliable. We reviewed training and certification data for 663 randomly selected guards in 6 of FPS's 11 regions maintained either in CERTS, which is the agency's primary system for tracking guard training and certifications, databases maintained by some regions, or contractor information. We found that 62 percent, or 411 of the 663 guards who were deployed to a federal facility had at least one expired certification, including for example, firearms qualification, background investigation, domestic violence declaration, or CPR/First Aid training certification. Without domestic violence declarations certificates, guards are not permitted to carry a firearm. In addition, not having a fully reliable system to better track whether training has occurred may have contributed to a situation in which a contractor allegedly falsified training records. In 2007, FPS was not aware that a contractor who was responsible for providing guard service at several level IV facilities in a major metropolitan area had allegedly falsified training records until it was notified by an employee of the company. According to FPS's affidavit, the contractor allegedly repeatedly self-certified to FPS that its guards had satisfied CPR and First Aid training, as well as the contractually required bi-annual recertification training, although the contractor knew that the guards had not completed the required training and was not qualified to stand post at federal facilities. According to FPS's affidavit, in exchange for a \$100 bribe, contractor officials provided a security guard with certificates of completion for CPR and First Aid. The case is currently being litigated in U.S. District Court.

FPS has limited assurance that its 15,000 guards are complying with post orders once they are deployed to federal facilities. 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. According to post orders, guards have many duties, including access and egress control, operation of security equipment, such as x-ray and magnetometer, detecting, observing and reporting violations of post regulations, and answering general questions and providing directions to visitors and building tenants, among others. We found that in the 6 regions we visited that guard inspections are typically completed by FPS during regular business hours and in cities where FPS has a field office. In most FPS regions, FPS is only on duty during regular business hours and according to FPS, LESOs are not authorized overtime to perform guard inspections during night shifts or on weekends. However, on the few occasions when LESOs complete guard inspections at night or on their own time, FPS has found instances of

guards not complying with post orders. For example, at a level IV facility, an armed guard was found asleep at his post after taking the pain killer prescription drug Percocet during the night shift. FPS's guard manual states that guards are not permitted to sleep or use any drugs (prescription or non-prescription) that may impair the guard's ability to perform duties.

Finally, we identified substantial security vulnerabilities related to FPS's guard program. Each time they tried, our investigators successfully passed undetected through security checkpoints monitored by FPS guards, with the components for an IED concealed on their persons at 10 level IV facilities in four cities in major metropolitan areas. The specific components for this device, items used to conceal the device components, and the methods of concealment that we used during our covert testing are classified, and thus are not discussed in this testimony. Of the 10 level IV facilities we penetrated, 8 were government owned and 2 were leased facilities. The facilities included field offices of a U.S. Senator and U.S. Representative as well as agencies of the Departments of Homeland Security, Transportation, Health and Human Services, Justice, State and others. The two leased facilities did not have any guards at the access control point at the time of our testing. Using publicly available information, our investigators identified a type of device that a terrorist could use to cause damage to a federal facility and threaten the safety of federal workers and the general public. The device was an IED made up of two parts—a liquid explosive and a low-yield detonator—and included a variety of materials not typically brought into a federal facility by employees or the public. Although the detonator itself could function as an IED, investigators determined that it could also be used to set off a liquid explosive and cause significantly more damage. To ensure safety during this testing, we took precautions so that the IED would not explode. For example, we lowered the concentration level of the material.¹³ To gain entry into each of the 10 level IV facilities, our investigators showed photo identification (state driver's license) and walked through the magnetometer machines without incident. The investigators also placed their briefcases with the IED material on the conveyor belt of the x-ray machine, but the guards detected nothing. Furthermore, our investigators did not receive any secondary searches from the guards that might have

¹³Tests that we performed at a national laboratory in July 2007 and in February 2006, demonstrated that a terrorist using these devices could cause severe damage to a federal facility and threaten the safety of federal workers and the general public. Our investigators obtained the components for these devices at local stores and over the Internet for less than \$150.

revealed the IED material that we brought into the facilities. At security checkpoints at 3 of the 10 facilities, our investigators noticed that the guard was not looking at the x-ray screen as some of the IED components passed through the machine. A guard questioned an item in the briefcase at one of the 10 facilities but the materials were subsequently allowed through the x-ray machines. At each facility, once past the guard screening checkpoint, our investigators proceeded to a restroom and assembled the IED. At some of the facilities, the restrooms were locked. Our investigators gained access by asking employees to let them in. With the IED completely assembled in a briefcase, our investigators walked freely around several floors of the facilities and into various executive and legislative branch offices, as described above.

Despite increased awareness of security vulnerabilities at federal facilities, recent FPS penetration testing—similar to the covert testing we conducted in May 2009—showed that weaknesses in FPS's contract guard training continue to exist. In August 2009, we accompanied FPS on a test of security countermeasures at a level IV facility. During these tests, FPS agents placed a bag on the x-ray machine belt containing a fake gun and knife. The guard failed to identify the gun and knife on the x-ray screen and the undercover FPS official was able to retrieve his bag and proceed to the check-in desk without incident. During a second test, a knife was hidden on a FPS officer. During the test, the magnetometer detected the knife, as did the hand wand, but the guard failed to locate the knife and the FPS officer was able to gain access to the facility. According to the FPS officer, the guards who failed the test had not been provided the required x-ray and magnetometer training. Upon further investigation, only two of the eleven guards at the facility had the required x-ray and magnetometer training. However, FPS personnel in its mobile command vehicle stated that the 11 guards had all the proper certifications and training to stand post. It was unclear at the time, and in the after action report, whether untrained guards were allowed to continue operating the x-ray and magnetometer machines at the facilities or if FPS's LESOs stood post until properly trained guards arrived on site.

FPS Has Recently Taken Some Actions to Better Protect Federal Facilities, However Many are Not Fully Implemented

While FPS has taken some actions to improve its ability to better protect federal facilities, it is difficult to determine the extent to which these actions address these challenges because most of them occurred recently and have not been fully implemented. It is also important to note that most of the actions FPS has recently taken focus on improving oversight of the contract guard program and do not address the need to develop a risk management framework and a human capital plan. In response to our covert testing, FPS has taken a number of actions. For example, in July 2009,

- 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 LESOs and guards. For example, FPS has recently issued an information bulletin to all LESOs and guards to provide them with information about package screening, including examples of disguised items that may not be detected by magnetometers or x-ray equipment. Moreover, FPS produced a 15-minute training video designed to provide information on bomb-component detection. According to FPS, each guard was required to read the information bulletin and watch the DVD within 30 days.

However, there are a number of factors that will make implementing and sustaining these actions difficult. First, FPS does not have adequate controls to monitor and track whether its 11 regions are completing these new requirements. Thus, FPS cannot say with certainty that it is being done. According to a FPS regional official implementing the new requirements may present a number of challenges, in part, because new directive appears to be based primarily on what works well from a headquarters or National Capital Region perspective, and not a regional perspective that reflects local conditions and limitations in staffing resources. In addition, another regional official estimated that his region is meeting about 10 percent of the required oversight hours and officials in another region said they are struggling to monitor the delivery of contractor-provided training in the region. Second, according to FPS officials, it has not modified any of its 129 guard contracts to reflect these new requirements, and therefore the contractors are not obligated to implement these requirements. One contractor stated that ensuring that its guards receive the additional training will be logistically challenging. For example, to avoid removing a guard from his/her post, one contractor plans to provide some of the training during the guards' 15 minute breaks. Third, FPS has not completed any workforce analysis to determine if its

current staff of about 930 law enforcement security officers will be able to effectively complete the additional inspections and provide the x-ray and magnetometer training to 15,000 guards, in addition to their current physical security and law enforcement responsibilities. Our previous work has raised questions about the wide range of responsibilities LESOs have and the quality of BSAs and guard oversight. According to the Director of FPS, while having more resources would help address the weaknesses in the guard program, the additional resources would have to be trained and thus could not be deployed immediately.

In addition, as we reported in June 2008, FPS is in the process of developing a new system referred to as the Risk Assessment Management Program (RAMP). According to FPS, RAMP will be the primary tool FPS staff will use to fulfill their mission and is designed to be a comprehensive, systematic, and dynamic means of capturing, accessing, storing, managing, and utilizing pertinent facility information. RAMP will replace several legacy GSA systems that FPS brought to DHS, including CERTS, Security Tracking System, and other systems associated with the BSA program. We are encouraged that FPS is attempting to replace some of its legacy GSA systems with a more reliable and accurate system. However, we are not sure FPS has fully addressed some issues associated with implementing RAMP. For example, we are concerned about the accuracy and reliability of the information that will be entered into RAMP. According to FPS, the agency plans to transfer data from several of its legacy systems including CERTS into RAMP. In July 2009, we reported on the accuracy and reliability issues associated with CERTS. FPS subsequently conducted an audit of CERTS to determine the status of its guard training and certification. However, the results of the audit showed that FPS was able to verify the status for about 7,600 of its 15,000 guards. According to an FPS official, one of its regions did not meet the deadline for submitting data to headquarters because its data was not accurate or reliable and therefore about 1,500 guards were not included in the audit. FPS was not able to explain why it was not able to verify the status of the remaining 5,900 guards. FPS expects RAMP to be fully operational in 2011, however until that time FPS will continue to rely on its current CERTS system or localized databases that have proven to be inaccurate and unreliable.

Finally, over the last couple of years we have completed a significant amount of work related to challenges described above and made recommendations to address these challenges. While DHS concurred with our recommendations, FPS has not fully implemented them. In addition, in October 2009, we plan to issue a public report on FPS key practices

involving risk management, leveraging technology and information sharing and coordination.

This concludes our testimony. We are pleased to answer any questions you might have.

Contact Information

For further information on this testimony, please contact Mark Goldstein at 202-512-2834 or by email goldsteinm@gao.gov. Individuals making key contributions to this testimony include Tida Barakat, Jonathan Carver, Tammy Conquest, Bess Eisenstadt, Daniel Hoy, Susan Michal-Smith, and Lacy Vong.

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

Statement on photography at the Department of Transportation headquarters
September 23, 2009
Erin McCann

Chairwoman Norton, members of the subcommittee, I'd like to thank you for the opportunity to speak to you today. I have a short statement, and then I'll be happy to answer your questions.

My name is Erin McCann and I am an amateur photographer. I am also an active member of a group called DC Photo Rights, which exists to document and discuss incidents in which photographers have been harassed by security officers or police.

In April, I became aware of a series of incidents at the Department of Transportation headquarters in Southeast DC during which security guards had stopped members of the public from taking pictures of the building. A photographer had written into a forum on the Washington Post Web site asking a columnist for help, and word of the incident spread through the DC photography community. Others shared their own similar incidents, and many headed to the building to see for themselves what would happen when they took their cameras out.

What we have documented since then is a series of incidents going back at least until 2007 during which security officers have stopped photographers for doing nothing more sinister than holding a camera on DOT property. I've attached the details of some of these incidents, including my own. It's important to note that this list is not exhaustive: for every incident someone shared, another photographer would chime in with agreement and say, "Yes, that happened to me there, too."

Many of the officers are polite, but they are firm in their belief that photography of the Department of Transportation, or any other federal building, is illegal. Others obscure their names, refuse to provide contact information for supervisors, threaten to confiscate cameras, and issue contradictory orders when questioned.

My own experience started on May 20. I phoned the DOT security office and spoke with a Lt. Hulse, who referred my call to a supervisor. When that supervisor failed to call me back by the end of the day, I decided to go to the building to see for myself what would happen. Soon I was standing in the lobby waiting for a supervisor, Lt. Butler, who, after taking down the details from my drivers' license, made the following points:

- When told that DOT seems especially zealous among federal departments in systematically training its guards to harass photographers, Lt. Butler said that makes him proud. He said DOT is doing it right, and everyone else is doing it wrong.
- Lt. Butler conceded that most of the people taking photographs of his building are harmless; the number he suggested was 90 percent. If I lived in the version of Washington where 10 percent of the people carrying around cameras were terrorists, I'd never leave home.
- Lt. Butler said his employees are trained to intercept all photographers, collect their contact information and forbid them from taking any more photographs of the building. This rule is an invasive attempt to collect personal data from law-abiding citizens. Thankfully, the security team often fails to collect such data from the people it stops.

After this conversation, I contacted the American Civil Liberties Union of the National Capital Area, which sent a letter to the DOT General Counsel's office on May 27 asking for an explanation. I've attached that letter to my testimony.

It took three months for the Department of Transportation to respond.

They apologized for my incident and said the guard was in error. They made no mention of the pattern of documented harassment, and there was no indication that any guards would be re-trained to end their systematic harassment of anyone with a camera.

By way of defending their attitude toward photographers, the DOT response included a 2004 Homeland Security bulletin regarding photography at federal buildings. It is a flawed document, claiming that a “widely known reconnaissance activity of criminal and terrorist organizations has been to gather photographic information about prospective targets.” In the age of Google maps and freely available satellite images, the idea that someone intending to harm a building needs first to conduct his own photographic reconnaissance is laughable. It’s also an embarrassing waste of everyone’s time.

The DOT is not unique in regarding photographers with suspicion. All around this city and the country, courthouses, train stations and federal office buildings have been deemed off-limits to people with camera. They do so under the mistaken belief that taking pictures in public places is illegal, or requires a permit, or is an indication that the person holding a camera is somehow a threat. In many cases, people have been detained, handcuffed and arrested for failing to move along when a guard tells them to. It is my belief that the time and energy spent questioning every camera-toting tourist could—and should—be put to a more constructive use.

Thank you.

Recent incidents at the Department of Transportation headquarters:

May 2007-present

The following links are photographs posted to Flickr by photographers who say they were approached by security officers around the Department of Transportation headquarters.

May 16, 2007: <http://www.flickr.com/photos/davetron5000/500730216/>

"The guard there said I was "not allowed" to take pictures on [government] property."

March 8, 2008: http://www.flickr.com/photos/chip_py/2318574865/

"While taking this photo a rather belligerent Department of Transportation cop came out and threatened to take my camera from me."

March 8, 2008: <http://www.flickr.com/photos/themosleyvault/2313215437/>

"It's actually quite depressing that a meaningless and dilapidated warehouse, that is over fifty yards from a government building, is actually worth protecting."

April 16, 2009: <http://www.flickr.com/photos/28181344@N00/3449280482/>

"I was questioned and asked for identification three separate times while attempting to photograph the Walk ... Throughout the experience, none of the security personnel with whom I spoke accurately described the law regarding photography in a public place. In fact, the first two quoted policy that was completely illegal."

April 25, 2009: <http://www.flickr.com/photos/spiggycat/3485136332/>

"The security guard started questioning me and my picture taking while we were sitting outside this starbucks in the corner Supposedly it is illegal (or at least not cool) to take pictures of federal buildings"

April 30, 2009: <http://www.flickr.com/photos/tonydefilippo/3489811457/>

"I was approached by a security guard at the Tingey Plaza behind the new DOT building in SE and asked why I was taking pictures (it was about 9pm on Monday night). The guard was polite but not the easiest to communicate with. I was polite and told him I was taking pictures for personal use only and was leaving the area when his supervisor came out and asked for my name and contact info."

April 15, 2009:

A participant on a washingtonpost.com chat wrote the following to columnist Marc Fisher:

Hi Marc, You were the first person I thought of after this happened. On Monday after the game, my husband, 1-year-old daughter and I were walking by the DOT building on our way to the car. They put in some new sculptures and signs along "Transportation Walk" -- specifically, three vintage gas pumps that were restored. My husband took a couple of photos of our daughter in front of one, but when he went to take a photo of another gas pump by itself, the security guard came up and told him that he was not allowed to take photos. There are no signs posted that prohibit taking photos there, and it's a public building. So why isn't he allowed to take photos there? Time for an organized protest?

Marc Fisher: Yes, absolutely--the only proven effective way to get these absurd anti-photography tactics stopped is to organize and protest. Effective letter-writing, publicity and civil disobedience campaigns have turned around such idiotic practices at Union Station, at the downtown Silver Spring shopping area, and in front of several federal government buildings. But you do need to embarrass them and confront them or the security guards will run roughshod over innocent tourists and photographers.

April 16, 2009:

Greater Greater Washington writer Stephen Miller posted this account (<http://greatergreaterwashington.org/post.cgi?id=2045>)

I was taking a photograph of an installation of vintage bicycles when a security guard some distance away yelled in my general direction. I couldn't understand what he said, so I pointed at myself to see if he was speaking to me but he made no further motion. I continued photographing until he approached me.

"What's going on here?" he asked.

"I'm photographing the bicycles," I replied. He continued walking, and I rode down to the next installation — three vintage gas pumps — and began taking photos of them.

"You can't do that here," he told me. I asked him why not. "It's the rules, for security," he said. I asked him what rule prevented me from taking photographs of public art, but he said that he could not tell me the rule. I asked if he worked for DOT or a subcontractor hired for security. "I can't tell you that," he replied again. I asked for his name, which he also refused to tell me.

"So you can't tell me the rule, your name, or who you work for?" I asked him.

"Nope," he replied. Luckily, at that point I was already done taking photographs, so I wished him a good evening and continued my ride.

I would raise this issue with the head of security at US DOT headquarters, but the guard refused to provide any information about who he works for.

May 20, 2009 (my incident):

I made a call to the Department of Transportation headquarters and spoke with a Lt. Hulse, who referred my call to a supervisor. When the supervisor failed to call me back by the end of the day, I decided to go to the building to see for myself what would happen.

I walked around the building once with the camera out and once more while actually shooting. Both times guards saw me and said nothing. It was only when I sat down near a guard shack that I saw an officer tell another man to put away his camera because photographing the building was not permitted.

When I asked her why she said that, she said it was simply what her supervisors told her to do. She immediately asked if I wanted to speak to one of them and directed me toward the building lobby where I would be met.

While waiting for the supervisor to arrive, the lobby guard confirmed what the first guard said, and also mentioned the possibility of terrorism. I confessed that I'd called earlier in the day and that I'd come to the building explicitly to see what would happen.

The supervisor, Lt. A. Butler, arrived and asked for my ID. When I hesitated, he immediately offered up his own and held it so I could write it down. He was in no way defensive while we chatted, and he was willing to stand there for an actual discussion.

In our 10-minute chat, the following points were made:

--When told that DOT is unique among federal buildings in DC in systematically training its guards to harass photographers, Lt. Butler said that makes him proud. His idea is that DOT is doing it right, and everyone else is doing it wrong.

--The second guard also pointed out that there are two buildings on Independence Avenue that are also on top of the photography threat, FAA and another one. When I ask where the FAA building is on Independence, he told me that if I don't know, he's not going to tell me. Hundreds of photos of this building are currently available online.

--Lt. Butler conceded that most of the people taking photographs of his building are harmless. The number he suggests is 90 percent, meaning 10 percent of the camera-wielding people nearby are potentially dangerous.

--He said the guards are trained to stop all photographers and collect their contact information. He said that photographers are not required to provide that data, and I failed to ask the obvious point of what would happen if a photographer refused. I said that in the interaction I witnessed before talking to him, the guard did not collect any information or engage the photographer except to tell him to move on. That, combined with a few other incidents I mention--like the one in which a guard threatened to take a photographer's camera--led him to suggest that there are some training issues that need to be resolved. He wants his guards collecting data from everyone they stop, and he wants them stopping everyone.

--I asked if now that he has collected my name and contact information I can be free to photograph the building. He said no, because, well, it's still illegal to photograph a federal building.

May 27, 2009:

The American Civil Liberties Union of the National Capital Area sends this letter to the DOT general counsel:



American Civil Liberties Union of the National Capital Area

1400 20th Street N.W., Suite 119 Washington, DC 20036-5920 202-457-0800

www.aclu-nca.org

Arthur B. Spitzer
LEGAL DIRECTOR

May 27, 2009

Rosalind Knapp, Esq.
Acting General Counsel
United States Department of Transportation
1200 New Jersey Ave, S.E.
Washington, D.C. 20590

Re: Alleged "no photography" rule outside the DOT building

Dear Ms. Knapp:

It has been brought to our attention that security officers at DOT Headquarters are routinely informing people that they cannot photograph the outside of the agency's building from nearby public places, and demanding identification from people who have taken such photographs. This appears not to be the mistaken actions of a few overzealous guards, but official policy. A supervisor, Lieutenant A. Butler, explained as much to a photographer a few days ago, according to the photographer's report to us.

We are not aware of any law that imposes such a rule, and we do not believe DOT has the authority to impose such a rule.

We would appreciate your checking into this and letting us know whether there is such a policy or practice. If there is such a policy or practice, we would like to know its source and whether you believe it is lawful. If there is no such policy or practice (or if there is such a policy or practice but you agree that it is improper), we would like to know that you have taken steps to disabuse the DOT security force of its mistaken beliefs and put an end to their harassment of the photographing public.

We look forward to your reply.

Sincerely yours,

Arthur B. Spitzer

August 19, 2009:

DOT finally responds to the ACLU letter.



U.S. Department of
Transportation
Office of the Secretary

General Counsel

1200 New Jersey Ave. N.E.
Washington, D.C. 20590

AUG 19 2009

Arthur D. Spitzer, Esq.
Legal Director
American Civil Liberties Union
of the National Capital Area
1400 20th Street, N.W.
Suite 1119
Washington, DC 20036-5920

Dear Mr. Spitzer:

I write in response to your letter of May 25, 2009 to our Deputy General Counsel, Rosalind Knapp, concerning whether the Department of Transportation has a policy or practice of prohibiting individuals from photographing the exterior of our buildings.

We do not, and in the instance that you discuss in your letter, our uniformed security guard was incorrect in telling the individual that he was not permitted to take photographs. For that, we do apologize.

As I say this, I hope you realize that the Department must operate under certain security strictures. Most pertinent to this situation is a Special Security Bulletin of the Department of Homeland Security's Federal Protective Service, a copy of which I enclose for your information.

Thank you for your patience in awaiting this response. Please let me know if you require any additional information.

Sincerely,

Ronald A. Jackson
Assistant General Counsel
for Operations

Enclosure



SPECIAL SECURITY BULLETIN

PHOTOGRAPHY OF FEDERALLY
OWNED AND LEASED FACILITIES

November 10, 2004



A. Overview:

Recent questions have been raised concerning the legality of photography on federally owned and leased property. The Federal Protective Service takes the protection provided to federal facilities, employees and customers very seriously, but that security concern must be balanced with the public's legitimate right to view and photograph federally owned and leased facilities. This bulletin provides guidelines to ensure the proper level of security is maintained for facilities and occupants without adversely impacting citizens' rights.

B. Guidance:

As a general, overarching guideline, the Federal Register, Vol. 67, No. 240, §102-74.420, provides that:

1. Except where security regulations apply or a Federal court order or rule prohibits it, persons entering in or on Federal property may take photographs of:

(a) Space occupied by a tenant agency for non-commercial purposes only with the permission of the occupying agency concerned;

(b) Space occupied by a tenant agency for commercial purposes only with written permission of an authorized official of the occupying agency concerned; and

(c) Building entrances, lobbies, foyers, corridors, or auditoriums for news purposes.

C. Discussion:

For properties under protective jurisdiction of the Federal Protective Service in the National Capital Region, there are currently no security regulations prohibiting exterior photography of any federally owned or leased buildings. It is important to note, however, that a widely known reconnaissance activity of

criminal and terrorist organizations has been to gather photographic information about prospective targets. As such, it is critical that law enforcement and security personnel be vigilant in carrying out the following proactive measures.

D. Implementation:

If individuals are identified taking photographs of the exterior of a facility, the following procedures should be followed:

1. Approach the individual or individuals taking the photographs.
2. Identify yourself.
3. Conduct a field interview to determine the purpose for taking photographs of the facility and endeavor to ascertain the identity of the individual.
4. If the field interview does not yield a reasonable belief of criminal behavior or terrorist reconnaissance activity, the photography should be permitted to proceed unimpeded.
5. If the field interview does yield a reasonable belief of criminal behavior or terrorist reconnaissance activity, immediately contact the Federal Protective Service Mega Center at (202) 708-1111.
6. All contact with the public, to include photographers, must be conducted in a professional but polite manner. Security personnel should not be distracted from their duties by engaging in assisting in the photographic effort.
7. Note that contract guards are only authorized to conduct security activities while on Federally owned or leased property. If the individual taking exterior photography of a Federally owned or leased facility is not physically located on property owned or leased by the Federal Government, the guard should immediately notify the Federal Protective Service Mega Center at (202) 708-1111 for a law enforcement response.

E. Conclusion:

Although it is legal to take photos and video of Federally owned and leased facilities, law enforcement and security personnel have an affirmative duty to carry out the protective measures above.

**ROBERT A. PECK
COMMISSIONER
PUBLIC BUILDINGS SERVICE**

U.S. GENERAL SERVICES ADMINISTRATION

BEFORE THE

**SUBCOMMITTEE ON ECONOMIC DEVELOPMENT,
PUBLIC BUILDINGS AND EMERGENCY MANAGEMENT**

**COMMITTEE ON TRANSPORTATION AND
INFRASTRUCTURE**

U.S. HOUSE OF REPRESENTATIVES

September 23, 2009



Good morning Chairwoman Norton, Ranking Member Diaz-Balart, and members of this Subcommittee. My name is Robert A. Peck and I am the Commissioner of the General Services Administration's Public Buildings Service (PBS). Thank you for inviting me to appear before you today to discuss GSA's role and expectations in the security of our facilities.

We have no more important responsibility than safeguarding our roughly one million Federal tenants, housed in GSA facilities, and their visitors in a manner that reflects the values of American democracy and the responsibility of our government to be open to the citizens it serves. Our buildings must be secure and at the same time must also be inviting and a good neighbor in their communities. This is a tall order.

GSA's PBS is one of the largest and most diversified public real estate organizations in the world. Our real estate inventory consists of over 8,600 owned and leased assets with nearly 354 million square feet of space across all 50 states, 6 territories, and the District of Columbia. Our portfolio is composed primarily of office buildings, courthouses, land ports of entry, and warehouses. GSA's goal is to manage these assets efficiently, while delivering and maintaining superior workplaces at best value to our client agencies and the American taxpayer. Achieving this goal requires a complete understanding of the threats facing our facilities, the accurate and timely identification of vulnerabilities, and a clear understanding of the tools available to us to overcome the vulnerabilities and counter the threats.

We rely on the Federal Protective Service (FPS) to conduct risk assessments of our facilities. These assessments and additional input from FPS help inform how we design, acquire, and run our buildings.

Like all executive branch agencies, GSA and FPS are subject to the security standards established by the Interagency Security Committee (ISC). The ISC's membership includes representatives from more than 40 Executive departments and agencies, in addition to the U.S. Courts.

GSA is the only federal agency whose mission is real property management that is represented in the ISC. Through our participation, we ensure that the real property perspective is included in all standards. Specifically, PBS engages representatives from all disciplines in developing our input: leasing specialists, architects, engineers, portfolio management professionals, customer service representatives, child care center specialists, and building management officials.

We are encouraged that the ISC is working to develop new standards that are moving in a direction that allows greater flexibility about risk-based allocation. At GSA, we firmly believe in the need for risk-based allocation of resources throughout our portfolio. Even in the area of physical security, this is particularly important. Funding and efforts must first be focused on the highest risk facilities, and against the highest risk threats.

GSA remains committed to providing our customers with a comprehensive work environment to allow them to complete their mission. We work continuously with FPS to assess, support, and safeguard our federal facilities. I met last week with FPS leadership in Kansas City to advance the risk-based allocation approach to security.

In closing, I'd like to reiterate that PBS is committed to providing our customers with the most effective working environments we can. Current standards dictate security measures that applied across a broad range of facilities. Integrating a new risk-based approach provides us with the most flexibility to address site specific conditions and balance necessary security measures with openness of our public buildings.

I look forward to working with the Committee as we continue to make great strides in this area. Thank you for allowing me to testify before you today. I welcome any questions you might have.

**Additional Norton QFRs
September 23, 2009 Hearing
“Risk-Based Security in Federal Buildings: Targeting Funds to Real Risks and
Eliminating Unnecessary Security Obstacles”**

1) Can the Process for getting on Schedule be streamlined and still held to a high standard?

GSA's Federal Acquisition Service (FAS) is currently managing several efforts to improve its processes that will afford better service to all its industry partners and customers. Several of these projects are outlined below. In addition, we would like to highlight ongoing support offered to small businesses to assist in the acquisition process. We feel very strongly that the Multiple Award Schedules program continues to be one of the lowest cost entries to federal contracting opportunities and that we continue to eliminate unnecessary barriers to entry.

The Multiple Award Schedules (MAS) program is one of the most successful contracting vehicles for small businesses. Over 80% of the nearly 18,000 MAS contracts are held by small businesses, and more than 35% of the more than \$38 Billion awarded to MAS contract holders goes to small businesses. These are direct awards, and do not reflect the additional dollars flowing to small businesses through large prime MAS contractors pursuant to their Small Business Subcontracting Plans.

FAS works closely with GSA's Office of Small Business Utilization to assist small businesses in navigating the Federal contracting landscape. Conferences, training events, one-on-one consulting sessions, and “How to Submit a Quality Offer” seminars are available across the country to provide assistance to small businesses seeking to obtain a MAS contract. **Pathways to Success** is an online tutorial intended to educate the contractor on all of the areas of contract compliance which need to be considered and addressed prior to deciding to pursue the submission of a Schedules contract offer.

FAS established a MAS Program Office to provide strategic direction, develop policy implementation guidance, ensure the alignment of acquisition systems with acquisition policy and business processes, and manage the process improvement efforts impacting the MAS program. FAS recently completed a review of the MAS solicitations focused primarily on professional services and standardized the solicitation provisions to as great an extent as possible. This will result in greater consistency in the information disclosure requirements and in the review process.

While striving to make the process for obtaining a MAS contract faster, easier, and more predictable, FAS is committed to maintaining the integrity of the offer review, evaluation, and award process. Customer agencies value the many pre-award responsibilities handled by GSA in awarding MAS contracts, allowing them to concentrate on managing the task order competition and making a best value determination. FAS has several

ongoing process improvement efforts targeted at streamlining the process to apply for and be awarded a Schedule contract. These efforts are outlined below:

e-Offer/e-Mod

This is a web-based tool which allows the contractor to submit their offer/modification electronically. The GSA contracting officer is able to review, evaluate, and make an award/no-award decision all within the system. Each party is required to have a digital certificate, and GSA has arranged to provide each contractor with two free digital certificates.

One of the key features of these systems is the ability to have the system quickly identify incomplete offers, thus reducing the tremendous amount of time currently expended by both Government and contractor personnel in correcting and amending various components of the offer which are incomplete. With the system "screening" offers, incomplete offers will not proceed to the Government contracting officer's desk, rather incomplete offers are returned to the contractor to allow for resubmission with the complete information required under the solicitation.

While these programs are currently voluntary on the part of the contractor, e-Offer and e-Mod will become mandatory features of the MAS program within the next two years.

RAM I/II

Rapid Action Mod (Phases I & II) will enhance the modification process to highlight and expedite the processing of those modification requests which by their nature require little effort. RAM I will allow for expedited processes for completing classes of administrative modifications. RAM II will allow for streamlined processing of modifications primarily adding new products to the schedule.

By identifying and streamlining the processing of these specific types of modifications, many modifications will be processed more quickly resulting in new products offered on the schedule faster, which is beneficial to contractors and the agency customer as well. Another result will be that contracting officers will have more time to be available to process the more complex actions such as new offers or complex modifications.

Because the RAM II implementation will require the contractor and the GSA contracting officer to reaffirm the Basis of Award and price/discount relationship established in the contract, GSA will always have a valid and current understanding of how the contractor takes its products and/or services to market. This will be a key aspect of another ongoing process improvement project to streamline the process of exercising Schedule contract options.

Formatted Pricelist

Currently, the contractor and the GSA contracting officer review the awarded pricing information both prior to award and then again when the contractor submits its electronic pricing file for upload to GSA Advantage.

The formatted pricelist will be a systems enhancement enabling the contractor to submit its electronic pricing file with its offer or modification request. Upon award, the pricelist file will be automatically uploaded to GSA Advantage. This will relieve the contractor from entering information into the GSA systems feeding GSA Advantage. Any pricing changes as a result of negotiations will be reflected in an amended pricing file submitted prior to award. An added benefit to this system change will be more accurate pricing in the GSA Advantage system.

Digitization Project

The digitization effort is a GSA-wide effort to move into a paperless office environment. Part of the effort involves the digitization of all contract files. This, combined with the full implementation of electronic contracting, will enable managers to shift workload across the nation as appropriate, view the status of each contract file, and respond with much greater knowledge to queries involving specific contract and programmatic issues and concerns.

Conclusion

While this is not an exhaustive list of the various initiatives which are expected to improve the ability to navigate the Schedules award process, they are the ones which will have the most immediate impact.

2) You mention on page 2 that there are 40 members on the Interagency Security Committee (ISC), but that GSA is the only agency whose mission is property management. Therefore I would expect GSA would be the Chair or at least have a unique leadership role on the ISC. How does GSA influence the ISC?

GSA holds a seat on the Executive Steering Subcommittee of the ISC, which guides and approves all ISC actions and planning. GSA co-chairs the ISC Standards Subcommittee, which ensures consistency between all standards, identifies needs for

updates and new standards, and resolves questions and confusion about existing standards.

GSA chairs the ISC Design Basis Threat working group and also chairs the ISC's Training Subcommittee. Furthermore, GSA holds seats on several ISC working groups that develop standards or guidance on contract guards, physical security criteria, and facility security committees. GSA intends to continue participation in several ISC working groups to ensure our unique understanding is considered in development of all new standards.

3) What is the GSA's cost estimate for protecting its inventory?

In Fiscal Year 2009 GSA paid FPS approximately \$50.6 million in basic and building specific charges for security and law enforcement services of GSA occupied and controlled space in our owned and leased inventory.

GSA provides additional funds to FPS via SWAs for the processing of background suitability determinations required for PBS and CHCO contract employees and for fire alarm and elevator monitoring services. The estimated costs incurred for these services provided in Fiscal Year 2009 were \$7.407 million and \$600,000, respectively.

GSA does not have knowledge of the value for SWAs received by FPS from other agencies.

WRITTEN STATEMENT

**JOHN D. PORCARI
DEPUTY SECRETARY OF TRANSPORTATION**

BEFORE THE

**COMMITTEE ON TRANSPORTATION AND INFRASTRUCTURE,
SUBCOMMITTEE ON ECONOMIC DEVELOPMENT, PUBLIC BUILDINGS
AND EMERGENCY MANAGEMENT
UNITED STATES HOUSE OF REPRESENTATIVES**

September 23, 2009

Chairwoman Norton, Ranking Member Diaz-Balart and Members of the Subcommittee, on behalf of the Secretary of Transportation Ray LaHood, thank you for inviting the Department here today to discuss the security practices and policies for the Department of Transportation headquarters located at 1200 New Jersey Avenue, S.E., Washington, D.C.

I am pleased to say that the Department of Transportation is enjoying its new headquarters building and we are excited to be a part of the redevelopment that is occurring in the Capital Riverfront area of Southeast Washington. We are also enjoying our proximity to the Nationals Baseball Stadium as well as the Navy Yard metro, which is just 400 feet from the Department's main entrance.

There was a strong commitment by DOT leadership to provide a safe and secure environment for its employees and to comply with post-9/11 recommended security measures in the design and construction of the facility to mitigate risks. The requirements for the DOT headquarters represented the Government's security consultants recommended industry practices, and were reviewed and adopted in collaboration with the Federal Protective Service and the General Services

Administration. The DOT headquarters security requirements were developed consistent with the prevailing Interagency Security Committee (ISC) Security Design Criteria; the General Services Administration policy guidance on fifty (50) foot setbacks issued in April 2002; and a detailed risk assessment and analysis conducted specifically for the Department that validated our requirements were appropriate for a cabinet agency with mission essential functions.

Under its lease agreement, the Government controls security at the DOT headquarters building. Based on a delegation of authority provided by the Department of Homeland Security through the Federal Protective Service, the Secretary of Transportation is solely responsible, without limitation, for protecting the DOT headquarters. This includes identifying building access requirements and procedures and monitoring the use of contract guard services. Security practices in DOT headquarters with respect to physical access control and visitor screening are consistent with other cabinet agency headquarters in Washington, D.C. Our security operations manage a uniformed security guard force that provides protection 24/7, to the DOT and Federal Aviation Administration headquarters buildings.

Madame Chair, DOT learned well the lessons of Oklahoma City, and was directly affected by the loss of valued employees in that senseless act of violence. Prior to the Oklahoma City bombing in 1995, there were no government wide standards for security at Federal facilities. Today, in our modern facility designed to the best available standards, the Department strives not only to provide a safe and secure environment for its employees, but also to be a good neighbor.

Our 5,900 employees support local business, and are part of the core of a bright and prosperous vision for the future of the Southeast waterfront. The Department has been recognized by the Capital Riverfront Business Improvement District for our efforts to be a good neighbor.

- We host a farmer's market open to all in the neighborhood every Tuesday in season.
- On Wednesdays at lunchtime, we host local musicians while vendors provide food and refreshments, and in the evening movies are shown behind our building for the benefit of neighborhood residents.
- Thursdays are open market days where local vendors can offer their wares.
- Beyond our daily good neighbor activities, we have also accommodated planned special events like the District of Columbia's Presidential Inaugural event which was held at DOT headquarters in January 2009.

The security practices and policies for the Department of Transportation headquarters building conform to Federal standards. Because of the new construction opportunity, we have been able to integrate post-9/11 security measures that have greatly enhanced the security posture of the DOT headquarters building compared to many existing government facilities and, we are grateful for that. Overall, the security practices and policies for the Department's headquarters building are equivalent to other cabinet agency headquarters here in Washington, D.C.

Again, thank you for the opportunity to testify before you today. I would be pleased to address any questions.

**COMMITTEE ON TRANSPORTATION AND INFRASTRUCTURE,
SUBCOMMITTEE ON ECONOMIC DEVELOPMENT, PUBLIC BUILDINGS, AND
EMERGENCY MANAGEMENT
UNITED STATES HOUSE OF REPRESENTATIVES**

**Risk-based Security in Federal Buildings:
Targeting Funds to Real Risks and Eliminating Unnecessary Security Obstacles
Hearing on September 23, 2009
Follow-Up Questions for Written Submission**

Questions from Congresswoman Eleanor Holmes Norton

Questions for Deputy Secretary Porcari:

1) How many employees are on the DOT building security committee? Do any have a strong security background?

The Department of Transportation (DOT) is the sole tenant in the three headquarters buildings (the Southeast Federal Center DOT Headquarters Building and the Federal Aviation Administration Headquarters - Federal Office Buildings 10.A and 10.B), and does not have a building security committee. The original building security committee concept was a recommendation in the Department of Justice (DOJ) Vulnerability Assessment Report published in June 1995 -- two months after the April 19th Oklahoma City bombing of the Alfred P. Murrah Federal Building. The intent was to provide a formal mechanism for addressing security issues at multi-tenant facilities controlled by the General Services Administration (GSA). The DOJ report envisioned a building security committee with representation from each of the federal agencies occupying the building, and a physical security specialist designated by GSA to provide security expertise.

In DOT headquarters, the physical security programs are managed by the Office of Security (OS) within the Office of the Assistant Secretary for Administration (OASA). The OS mission is to ensure the safety, security, and protection of DOT personnel, information, facilities, and other assets. The OS staff includes experienced individuals who are qualified GS-080 Physical Security Specialists. The head of OS is a Senior Executive required to have extensive security management experience. Major decisions for security measures in DOT headquarters are coordinated internally through an Administrative Management Council that includes representation of all elements of DOT and are largely funded from a DOT Working Capital Fund that is managed by OASA.

2) What is the security policy regarding use of the garage? Does that change on the weekends?

The headquarters parking garages are situated below grade and within the buildings' perimeters. The headquarters parking garages are under 24 hour access control by the Government and no parking of third party vehicles is allowed. The DOT headquarters admittance policy permits only holders of a valid DOT-issued identification card to enter a

garage at a DOT headquarters building. Vehicles displaying a parking permit may enter the garage for the period (month, day, or time span) authorized by the permit. Visitor vehicle parking is not authorized. The DOT security policy for the parking garages does not change on the weekends.

3) Within 30 days, please provide to the Subcommittee a procedure in place for looking at current training and your plans to consult and revise those procedures as necessary.

The Department of Transportation's (DOT) armed guard services contractor has an Annual Training Program (ATP) for its contract Security Force that covers multiple training requirements. The total projected training for fiscal year 2009-2010 is over 11,600 hours. The training is conducted to meet the standards of the Federal Protective Services information manuals for contract guards and contract security. The training program has several components that cover policy, procedural, and tactical training requirements, including:

- Basic Contract Guard Training (72 hours minimum)
- Firearms Training (40 hours minimum)
- Adult, Infant and Child CPR and First Aid Training
- Baton, Handcuffing and Other Tactical Training
- Protective Mask Training for Nuclear, Biological, Chemical Incidents
- Orientation Training on the Roles of Law Enforcement Officers (40 hours minimum)
- Physical Fitness Training
- Officer On-the-Job (OJT)/New Hire Training (40 hours)
- Biennial Re-certification Training (40 hours minimum)

The DOT Office of Security monitors Federal security guidelines to ensure that the contractor's Annual Training Program is up to date and provides the security workforce with any new or revised training or instruction that are needed to improve the security practices in DOT headquarters. In this way, DOT is achieving its objective to have a highly trained and qualified Security Force.

With respect specifically to exterior photography, DOT has revised its security procedures and established new training requirements to address the issues raised in the September 23rd hearing. In late September, DOT consulted with the Department of Homeland Security's Federal Protective Service and General Services Administration. There were no expressed objections to DOT modifying its procedures to eliminate the field interviews that are conducted when a person is found to be photographing a Federal facility. In October, DOT required the contractor to conduct training for the guard force to review the rights of photographers and provide instructions to begin detecting, monitoring, and reporting, but not interviewing, persons taking photographs of the exteriors of DOT headquarters buildings. If the DOT guard force observes suspicious circumstances, they will immediately notify the FPS rather than conduct a field interview. After the guards were instructed regarding this change in procedure, they were required to certify a sheet outlining the new DOT Photographer Observing and Reporting Procedures. Also, the contractor updated the New Hire OJT training packet to add the new procedures eliminating the field interview.

Obrock, Michael

From: Luther, Margaret <CTR> [Margaret.Luther@associates.dhs.gov] on behalf of I&A Exec Sec [I&AExecSec@hq.dhs.gov]

Sent: Friday, November 06, 2009 7:23 AM

To: Brita, Susan; Obrock, Michael

Cc: I&A Exec Sec; Atkins, Miranda; Delawter, Denise

Subject: 0911-05-0477: ECT 846124 - Risk-based Security in Federal Buildings
Susan and Michael,

I&A received a request to review QFRs on *Risk-based Security in Federal Buildings: Targeting Funds to Real Risks and Eliminating Unnecessary Security Obstacles*. After reviewing the QFRs, I&A has no comment. We have added a step note in ECT/IQ recording such and, at the request to send final responses to you, are also sending an email confirming a no comment by I&A.

If there are any questions, please feel free to contact I&A Exec Sec at the numbers listed below.

Regards,
~Maggie

*Margaret Luther
Department of Homeland Security
Office of Intelligence and Analysis
Executive Secretariat Office
202-447-4269/202-282-9149*

11/18/2009



STATEMENT

OF

**GARY W. SCHENKEL
DIRECTOR, FEDERAL PROTECTIVE SERVICE
U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT
U.S. DEPARTMENT OF HOMELAND SECURITY**

REGARDING A HEARING ON

***“Risk Based Security: Targeting Funds to
Real Risks and Eliminating Unnecessary Security Obstacles”***

BEFORE THE

U.S. HOUSE OF REPRESENTATIVES

COMMITTEE ON TRANSPORTATION AND INFRASTRUCTURE

**SUBCOMMITTEE ON ECONOMIC DEVELOPMENT,
PUBLIC BUILDINGS AND EMERGENCY MANAGEMENT**

Wednesday, September 23, 2009 – 2:00 p.m.

2167 Rayburn House Office Building

WASHINGTON, DC

INTRODUCTION

Chairwoman Norton, Ranking Member Diaz-Balart, and distinguished members of the Subcommittee, thank you for the opportunity to appear before you today to discuss the Federal Protective Service (FPS). I look forward to discussing FPS' mission as well as describing the steps we have taken to address the concerns raised recently by the Government Accountability Office (GAO).

FPS BACKGROUND

As I have testified previously, FPS delivers integrated law enforcement and physical security services to Federal agencies in almost 9,000 facilities owned and leased by the General Services Administration (GSA) throughout the United States and its territories. FPS performs fixed-post access control, implements screening functions, and provides roving patrols of facility perimeters and communal open space. FPS is comprised of 1,225 Federal law enforcement and support staff personnel. FPS also leverages more than 15,000 contract security guards employed by private companies to supplement its physical security services.

FPS Law Enforcement Security Officers (LESO), also called inspectors, are uniformed law enforcement officers who possess the authority and training to perform traditional police functions. Currently, FPS has approximately 600 inspectors, who are trained as physical security experts that provide comprehensive security services such as Facility Security Assessments and implementation and testing of security measures.

As you know, to serve customer agencies (tenant agencies) in federal facilities, FPS must effectively balance the need for security with the need for ready public access to government services. This means that FPS, in conjunction with the agencies that

occupy the facilities, must provide security solutions that ensure a safe and secure environment and that do not deter people from conducting regular business.

FPS offers comprehensive physical security operations; installs security systems (alarm systems, X-rays, magnetometers, and entry control systems), monitors those systems 24 hours a day, seven days a week; and provides uniformed police response and investigative follow-up. The provision of contract security guard services, crime prevention seminars tailored to individual agency and employee needs, facility security surveys, integrated intelligence gathering and sharing, and special operations capabilities are all part of the broad FPS mission.

FPS annually conducts nearly 2,500 Facility Security Assessments and responds to approximately 1,400 demonstrations. In Fiscal Year (FY) 2008, FPS responded to 2,571 protests and organized disturbances, made 1,888 arrests, investigated more than 2,100 accidents, investigated 1,503 larcenies, processed 248 weapons violations, and prevented the introduction of 669,810 banned items into federal facilities. Of the approximately 9,000 buildings protected by FPS, 1,500 are categorized as Security Level III or IV (highest risk buildings).

CHALLENGES AND PROGRESS

Upon my arrival in April 2007, it was apparent FPS was experiencing some serious challenges. The agency transferred from GSA to DHS in 2003 with a full-time equivalent (FTE) workforce of over 1,400 spread across the country into 11 regions, and I saw that FPS needed to focus on becoming a single, standardized organization. This required a new operational construct and new business practices. However, FPS simultaneously faced budget constraints due, in part to poor financial and contract management, as well as fee collections requested in the President's FY 2008 budget that

supported fewer personnel than were on board at the time the budget was sent to the Congress. To avoid having to reduce the number of federal employees, FPS sought to realize savings in other areas. Consequently, many programmatic elements such as training and equipment purchases had to be rescheduled until such time that FPS could determine that it had sufficient funding. FPS of course remained obligated and dedicated to protecting almost 9,000 GSA-owned and leased facilities, overseeing 15,000 armed contract security guards and managing over 150 contracts.

During this period, FPS carefully assessed its organization and made difficult decisions. This refocusing effort culminated in the development of a strategic plan to shape future activities (published 2008). FPS now focuses on critical issues within its protective mission and is developing a sound strategic path forward focused on facility security and the safety of the occupants of and visitors to those facilities.

In particular, FPS focused on standardizing best financial practices. Evidence of FPS's success was the 2007 Invoice Consolidation project that paid 2,200 past due invoices, some of which dated back to 1999, and reduced financial loss via prompt interest payments. This effort resulted in over \$1 million in savings in 2008.

The 2008 Consolidated Appropriations Act created a staffing baseline for FPS by requiring a workforce of no less than 1,200 federal FTEs and the authority to raise fees to financially support that number. FPS increased its basic building security fee, and, as a result, in March 2008, embarked on its first hiring effort in more than six years. FPS now has 1,236 FTEs. Providing our workforce with the appropriate skills in the appropriate geographic locations continues to be paramount on our task list and will underpin our comprehensive Mission Action Plan.

We also are focused on providing greater training to our entire security guard workforce and I will touch on the steps taken to improve training a little later in my

testimony. We are dedicated to our mission, to our profession, and to improving our organization's execution of this extremely important mission.

Further, the transfer of FPS from U.S. Immigration and Customs Enforcement (ICE) to the National Protection and Programs Directorate (NPPD) requested in the President's FY 2010 Budget will provide DHS with a single component responsible for a comprehensive infrastructure security program. The integration of FPS into NPPD enhances DHS' overarching strategy and mission to lead the unified effort to improve our nation's security.

RESPONSE TO GAO'S FINDINGS

Within 24 hours of being notified of the GAO report dated July 8, 2009, titled "*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), FPS took the following actions:

- Established a national study group to examine FPS' visitor and employee screening processes;
- Directed FPS Regional Directors to exercise recently established overt and covert inspection techniques to assess, verify, and validate the various elements of employee and visitor screening processes;
- Required Regional Directors to institute random searches as part of visitor and employee screening procedures;
- Instructed Regional Directors to immediately increase oversight and inspection of contract guards and authorized overtime pay to accomplish and sustain this increased tempo;

- Instructed FPS employees to be constantly vigilant and to immediately report any observation of poor performance of duties of the contract guard force to FPS law enforcement personnel or their supervisors;
- Advised guard contractors in a letter that substandard performance of contract guards is unacceptable and will not be tolerated, and put them on notice that the number and frequency of guard post and certifications inspections will increase;
- Issued an Information Bulletin to all inspectors and security guards to reinforce training techniques and to provide them with information about screening packages, including examples of disguised weapons and components of improvised explosive devices (IEDs); and
- Provided information pertinent to the situation to all FPS stakeholders, including client/tenant agencies, regarding the incident and actions being taken in letters signed by the Director of FPS.

A team of people, both internal and external to FPS (including leadership from FPS, the Transportation Security Administration, U.S. Marshals Service, and senior DHS personnel), is now working diligently to implement meaningful and lasting solutions to deliver on these immediate actions.

FPS already has taken many steps to improve the visitor and employee screening process at federal facilities, including improved training of contract guards and oversight of those guards. These steps are summarized below:

- FPS had already addressed all of the specific personnel misconduct identified in the GAO report. In all cases, the employee or guard in question was removed from FPS contracts. With regard to the security breaches involving IED components, GAO still has not identified the specific location of the breaches. As

noted below, however, any such breaches will be dealt with by across-the-board increased training, improved oversight, and fortified inspection policies.

- To ensure FPS contract guards have the training required to identify component parts of an IED, FPS issued a training bulletin to all contract guards about proper screening methods and situations indicative of a possible concern. FPS has confirmed that each contract guard company has confirmed that all of their guards have received the bulletin.
- All contract security guards' certification and qualification records have been reviewed and updated. FPS also has met with each guard company to review protocols and continued communication with contract guard companies to impress upon them the importance of valid certifications.
- Regional Directors have increased the frequency and quantity of certification inspections with contract guard companies.
- FPS has completed filming of a training video, which was sent to all guard companies during the week of August 31. A contract modification has been made where necessary to ensure guard companies are required to certify when the video has been viewed by the guards. This video addresses how to screen for possible component parts of an explosive device and detect situations that warrant additional screening and questioning. As of September 17, 74.11 percent of guards had certified viewing; by the end of this current week, any guard company that has not achieved 100 percent viewing will be required to submit a completion plan.
- On September 16, 2009, FPS continued its efforts in training its members and contract guard force by issuing a specific Training Bulletin regarding Peroxide-

based Homemade Explosives in light of recent developments involving terrorist activity identified by the Federal Bureau of Investigation (FBI).

- FPS has increased the frequency of guard post inspections and, based on availability of funds, anticipates maintaining this operational tempo. FPS has been deploying uniformed and plain-clothed FPS officers to inspect posts. In addition, FPS has increased around-the-clock random inspections.
- By the end of July, FPS reviewed and updated certification and qualification records for 100 percent of its contract security guard force. Not only was the information updated, it was also validated to ensure that every contract security guard has the qualifications and certifications required for his or her position. FPS immediately notified, and will continue to notify, individual contract security guards and the contract security guard company of any lapses. FPS will also provide instructions for corrective actions and consequences for not complying with those actions.
- FPS has established a Covert Testing Working Group (CTWG) to enhance and complement the ongoing efforts to improve FPS' operational oversight of the contract security guard program. Covert testing is already being done. However, the CTWG will establish a national covert testing program and determine a national schedule for testing facilities. The standardized testing kits are in procurement process and should be available within 90 to 120 days. The CTWG Policy is in draft stage and will be ready for signature within 90 days, and the first CTWG teams will be deployed within the 2nd Quarter of FY 2010. The formalized process of the CTWG will be complete and deployed within 180 days.
- Over the last year, FPS developed and implemented five new policies to strengthen its oversight of the contract guard program. These policies will

improve the contract award process and establish the frequency of inspections of guard posts. As guard post inspections are critical, the inspection policy prioritizes facilities based on risk.

- Even prior to the recent GAO report, FPS has assessed monetary deductions for personnel performance violations, including the failure to maintain proper certifications. In March 2008, FPS terminated for default a contract with a guard company for having various guards standing post with improper or fraudulent certifications.

In addition to all of those actions, I believe that more work is needed to improve the training of contract guards, and additional study is required to determine whether contract guards are maintaining constant vigilance. To that end, FPS is taking steps to bolster training and performance, increase oversight and supervision (including in the form of covert inspections), and create a more uniform protection system:

1) FPS has and will continue to receive and consider recommendations from the recently established national Tiger Team led by experienced FPS regional directors to critically examine FPS' visitor and employee screening processes.

2) FPS has developed a national training plan to train or re-train contract security guards on X-ray machines, magnetometers, and IED detection. The program: will standardize screening procedures and contract guard training across FPS; will be designed to increase the ability of FPS contract security guards to detect and prevent the introduction of suspicious items, weapons, and bomb components using x-ray and magnetometer technology; and will create a cadre of x-ray and magnetometer instructors who will be capable of delivering X-ray and magnetometer screening training to the contract security guards in each FPS region.

3) FPS is completely revising the system used to ensure that contract guards have the required training and certifications. In addition, certification and training information will be monitored using the Risk Assessment and Management Program (RAMP) to revolutionize the Facility Security Assessment (FSA) process and replace the six disparate systems currently used by our inspectors. RAMP will electronically notify each contract guard company of the status of each guard's certifications and qualifications as well as post inspections. If there is a lapse, the company and the supervising FPS inspector will be notified that the guard may not perform work on the contract. RAMP should be operational by November 2009.

4) FPS is also developing the Computer Aided Dispatch and Information System (CADIS), which will standardize reporting procedures, consolidate crime and incident reporting, and time stamp our operations, thus providing accurate, data-driven support for future staffing models. We anticipate CADIS being online in FY 2010.

5) In FY 2010, FPS will procure a Post Tracking System (PTS) to ensure uncertified or improperly certified guards do not stand post. This will function as an automated timekeeping system for contract security guards. The system will not allow a disqualified guard to "clock in" and the guard company will receive notice that the post is thus unmanned. PTS will improve the accuracy of post staffing and billing and will further reduce the administrative burden on our inspectors, allowing them more time for active patrol and guard oversight.

6) FPS continues to examine if it has the proper mix of staffing. For example, FPS determined it will staff 11 vacant Regional Training Coordinator positions with temporary promotions until permanent selections can be made. FPS has selected and installed a Director for the Policy, Compliance and Audit Directorate to ensure that

policies and procedures governing oversight of the contract security guard force are not only standardized and implemented, but also result in the highest degree of protection of federal facility occupants.

7) FPS has awarded a national contract to increase national Explosive Detector Dog teams to 75 (currently staffed at 51). The first additional trainees report to Auburn University for training this month.

8) FPS will continue to increase random searches of packages, briefcases, and bags as part of visitor and employee screening procedures and ensure that signs are posted alerting those entering the building that they are subject to these searches.

9) FPS delivers recurring messages to FPS employees and other stakeholders to be constantly vigilant and to immediately report poor performance or suspicious activity.

10) FPS will continue dialogue with the DHS Science and Technology Directorate, Transportation Security Administration, the Office of Infrastructure Protection, and the U.S. Marshals Service to explore the possibility of developing and deploying new technologies, as well as training opportunities to improve the execution of FPS' mission.

11) FPS will replace X-ray machines with improved X-ray technology. FPS recently awarded a \$25 million, five-year blanket purchase agreement to lease new advanced X-ray machines.

CONCLUSION

After reviewing the problems identified by GAO, I believe the steps outlined above will redress those problems, and the proposed future steps will ensure the improved protection of the nearly 9,000 GSA owned and leased buildings protected by

the FPS workforce and contract guards. In addition, Chairwoman Norton, I applaud your leadership role in the effort to strike the right balance between security and access to our federal buildings, and look forward to working with you and this Subcommittee on addressing those challenges.

I want to express to you my personal sense of urgency and commitment to the important responsibility I share with the men and women of FPS in keeping our nation safe. I am honored to lead the proud and professional men and women of FPS. I can tell you that they are dedicated, determined and committed to developing, implementing, and maintaining the highest level of physical security to ensure that the facilities they are charged with protecting are secure and that their occupants are safe.

Thank you again, Chairwoman Norton and Ranking Member Diaz-Balart, for holding this important oversight hearing. I would be pleased to answer any questions you may have.

Question#:	1
Topic:	actions
Hearing:	Risk-based Security in Federal Buildings: Targeting Funds to Real Risks and Eliminating Unnecessary Security Obstacles
Primary:	The Honorable Eleanor Holmes Norton
Committee:	TRANSPORTATION (HOUSE)

Submitted by Department of Homeland Security - FPS

Question: Mr. Schenkel, given the very serious nature of GAO's recent security breach of several federal buildings, what specific actions have you done to address, for example, the policy of liquids coming into federal buildings, more visual inspections, etc. Have you changed policy? Have you ramped up the role of FPS on building security committees?

Response: FPS developed a standardized 16-hour training module of additional guard training for regional implementation. FPS partnered with the U.S. Marshals Service and the U.S. Secret Service to develop the most updated training curriculum available. FPS has completed the initial train-the-trainer for hand-selected FPS field personnel. These trained inspectors are currently in the various FPS regions implementing the additional 16-hour module of training which is specifically designed to enhance the guards' ability to detect components of improvised explosive devices using the X-ray and Magnetometer. This 16-hour module is in addition to the 16 hours of X-ray and Magnetometer training that contract security guards receive in their initial training. FPS anticipates full implementation of the standardized training by January 2010.

FPS is addressing the proper use of screening equipment, screening procedures, and overall education on potential threats rather than focusing strictly on liquids. FPS has also published three additional training bulletins, produced a training video, and modified guard contracts to ensure 100 percent compliance with this essential guard training.

The Federal Management Regulations (FMR) Sections 102-74.435 and 102-74.440 prohibit explosives and weapons in Federal buildings. The Facility Security Committee (FSC) may choose to prohibit other items from a specific facility. FPS cannot enforce a ban on liquids entering federal facilities unless the FSCs elect to establish such a policy. Since FPS is not a voting member of the FSCs, it can only influence the decisions of the FSCs through professional representation of identified risks and recommendations of appropriate countermeasures. FPS continues to serve as an active participant and resource for FSCs.

Question#:	2
Topic:	CERTS
Hearing:	Risk-based Security in Federal Buildings: Targeting Funds to Real Risks and Eliminating Unnecessary Security Obstacles
Primary:	The Honorable Eleanor Holmes Norton
Committee:	TRANSPORTATION (HOUSE)

Question: What steps have you taken to ensure the Contract Guard Employment Requirements Tracking System (CERTS) is more reliable?

Response: To immediately correct the data in CERTS, I ordered a review of all guard certifications. In addition, each FPS Regional Director was tasked with providing FPS headquarters up-to-date and accurate information on all active contract security guards, which involved not only collecting and compiling all of the certification and qualification information to be entered into CERTS, but also validating it to ensure that required certifications (inclusive of training, weapons qualifications, examination score, and suitability) were current.

On July 24, 2009, each Regional Director submitted information that will undergo a continuous data-level quality assurance review by headquarters information technology staff prior to being uploaded into CERTS. We are currently performing Operation Shield and increasing the frequency of inspections. This information will be uploaded into CERTS, and all regions will be required to continuously review, update, and correct any identified discrepancies. The information in CERTS will be reviewed daily for accuracy. Verifiable information will be migrated into the FPS Risk Assessment and Management Program (RAMP) in November 2009. RAMP will allow FPS inspectors and analysts access to up-to-date, real-time information on the certification requirements of contact guards.

Question#:	3
Topic:	policies
Hearing:	Risk-based Security in Federal Buildings: Targeting Funds to Real Risks and Eliminating Unnecessary Security Obstacles
Primary:	The Honorable Eleanor Holmes Norton
Committee:	TRANSPORTATION (HOUSE)

Question: What are the 5 new policies you have put in place to strengthen oversight on guards?

Response: There are more than five new policies in place. We have undertaken a comprehensive program by which we have developed and issued national policies that have led to the standardization of business processes, which includes the implementation of 26 policies (eight of which are on guard oversight (listed below)).

FPS has established a Policy, Compliance and Audits Directorate to (1) work with subject matter experts in the field and at headquarters to develop additional policies, and (2) ensure regional compliance with these policies by conducting cyclical program inspections. We are enhancing our ability to train FPS personnel on new policies via a variety of training venues, including webinars, on line computer-based courses, and on-the-job training. We also have added rating factors to the performance plans of regional directors to hold them accountable for ensuring that they and their personnel comply with national directives and SOPs. They are:

15.9.1.1, Security Guard Acquisition Planning and Pre-award: This directive establishes standardized requirements for, and organizational responsibilities of, the FPS Security Guard Acquisition Planning and Pre-award process. This directive improves oversight by standardizing roles and responsibilities of employees engaged in acquisition planning for contract security guard services.

15.7.2.5, Operation Shield: This directive establishes FPS policy, standards, responsibilities, and procedures for Operation Shield, which tests contract guard proficiency and compliance with post orders, policies, and procedures.

15.5.1.5, Initial Offense and Incident Case Reporting: Establishes the requirements for incident reporting by FPS law enforcement officers and security guards. This directive improves oversight by standardizing contract security guard reporting of Part III offenses which include security, assistance, and miscellaneous incidents of a non-criminal nature.

09-001, Guard Contract Performance Monitoring Program: Establishes policy for monitoring the performance of FPS's contract security guards, guard forces, and

Question#:	3
Topic:	policies
Hearing:	Risk-based Security in Federal Buildings: Targeting Funds to Real Risks and Eliminating Unnecessary Security Obstacles
Primary:	The Honorable Eleanor Holmes Norton
Committee:	TRANSPORTATION (HOUSE)

contractor management functions. It also assigns organizational responsibilities for post, site, and administrative inspections and annual contractor performance evaluations.

08-003 , Contract Guard Post Desk Book Program: Establishes the FPS contract guard post desk book program and assigns organizational responsibilities for the development, management, and administration of standardized post desk books for all contract security guard force activities.

08-007, Oversight of Contractor-Provided Training: This directive establishes policy and procedures for FPS monitoring and oversight of the performance of contractors who provide contract required security guard training.

08-008, Contract Guard Written Examination Program: Establishes the policy and procedures requiring contract security guards to pass a written examination in order to work on an FPS contract.

07-005, Agency Technical Representative Program: This directive establishes the roles and responsibilities for the assignment and use of agency technical representatives to provide limited, on-site, contract and operational oversight for the contract guard program.

Question#:	4
Topic:	x-ray
Hearing:	Risk-based Security in Federal Buildings: Targeting Funds to Real Risks and Eliminating Unnecessary Security Obstacles
Primary:	The Honorable Eleanor Holmes Norton
Committee:	TRANSPORTATION (HOUSE)

Question: You mention leasing advanced X-ray machines. I assume there are no funds to purchase the equipment. What is the anticipated cost of the rentals? How would be the purchase price?

Response: In fiscal year 2009, FPS established the National Countermeasures Program to standardize and ensure the consistency of countermeasures at all of the facilities that FPS is responsible for securing and protecting. Initial review of the countermeasure equipment, primarily X-ray machines and Magnetometers, resulted in the development of national contracts to ensure that the equipment being deployed by FPS met the standards and requirements for access control and package screening. The inventory of existing equipment was updated and replacement schedules established based on estimated useful equipment life-cycles. A statement of requirements was prepared and market surveys were conducted to determine the most effective and efficient acquisition strategy to fill these needs.

Based on the information received relative to the physical size and weight of the units, the technical complexity of the hardware and software, the large initial cost, and the cost of environmental mitigation at the time of disposal, the decision was reached to acquire X-ray machines using a fully-loaded lease acquisition, to include shipping, delivery, installation, initial training, maintenance, and disposal. The lease option eliminates the administrative burden and related separate acquisitions for operation, maintenance, installation, and disposal. It also ensures that the X-ray machines are replaced timely at the end of their useful life-cycle.

Over the full period of the lease (base year plus four option years), the cost to lease the machines used for screening personal items (small X-ray machine, used at building entrances) is approximately \$27,000 compared to \$46,000 to purchase them. The cost to lease the machines used to screen packages (large X-ray machine, used at loading docks), over the five year period of the lease is approximately \$36,000, while the cost to purchase is \$63,000.

As stated above, the lease agreement includes regular maintenance and early replacement of the machines if necessary. These maintenance costs also include any parts and labor that are required to conduct regular maintenance or repairs. Had this equipment been purchased outright, the maintenance fees for both types of machines would total approximately \$36,000 over the five year lease period. Accordingly, the lease costs

Question#:	4
Topic:	x-ray
Hearing:	Risk-based Security in Federal Buildings: Targeting Funds to Real Risks and Eliminating Unnecessary Security Obstacles
Primary:	The Honorable Eleanor Holmes Norton
Committee:	TRANSPORTATION (HOUSE)

compare favorably with the direct cost of purchasing the X-ray machine and the separate costs for installation, operation, maintenance, and disposal over the same period. Had the analysis determined that purchasing the X-ray machines was more advantageous than leasing, funds would have been available to support that decision. In FY 2009, 298 X-ray machines were ordered at a cost of \$3,457,505.

Using similar criteria, the decision was made to purchase Magnetometers using a national blanket purchase agreement and establish a separate national maintenance contract. In both cases, FPS believes that its acquisition strategies are the most effective and efficient method of meeting the security equipment needs of our customer agencies that ultimately pay for the equipment in the FPS monthly security bill.

Question#:	5
Topic:	model
Hearing:	Risk-based Security in Federal Buildings: Targeting Funds to Real Risks and Eliminating Unnecessary Security Obstacles
Primary:	The Honorable Eleanor Holmes Norton
Committee:	TRANSPORTATION (HOUSE)

Question: Why can't FPS set up a model similar to the TSA model which really standardized security in all airports?

Response: Each GSA facility has an established Facility Security Committee (FSC), comprised of tenant agencies with varying levels of security experience, which retains the authority to implement countermeasures recommended by FPS. FPS must abide by the decisions of the FSCs. The FSCs, whose contracts fund FPS, determine the access control procedures that will be enforced by FPS security guards protecting each facility.

Since the chairperson of each FSC is in most cases a representative of the largest tenant of a facility, they have the most influence in accepting or rejecting an FPS recommendation for countermeasures or screening procedures/processes. Many times the tenants have to weigh the benefits of providing funding to enhance the security of the facility versus a programmatic use of funds. It becomes a difficult task to balance the requirements and needs for the tenants collectively. Additionally, agencies typically submit budgets years in advance. In the event that FPS makes a recommendation for a new countermeasure based on the Interagency Security Committee's (ISC) Federal Security Level (FSL) schedule in an out year, the agencies may have to redirect funds from other programs to emplace a recommended countermeasure.

Question#:	6
Topic:	RAMP
Hearing:	Risk-based Security in Federal Buildings: Targeting Funds to Real Risks and Eliminating Unnecessary Security Obstacles
Primary:	The Honorable Eleanor Holmes Norton
Committee:	TRANSPORTATION (HOUSE)

Question: What is the status of the Risk Assessment Management Program (RAMP)?

Response: The first phase of the FPS Risk Assessment and Management Program (RAMP) was released on November 16, 2009. The initial phase will streamline FPS operations and increase FPS's ability to provide robust security services for federal facilities. Most importantly, RAMP will provide a single source of information to manage physical security for the facilities FPS protects.

Comprehensive training for FPS inspectors, area commanders, federal police officers, and others began on October 16, 2009. The training for RAMP includes 80 hours of instruction that is being delivered over two weeks and has been designed to cover not only the functionality of the system, but also provide participants with an in-depth understanding of updated risk assessment practices and the methodology used by RAMP. Concurrently, FPS personnel are also being issued the ruggedized laptops that they will use as their single computing platform to analyze information on facilities and applicable risks.

Question#:	7
Topic:	DOT
Hearing:	Risk-based Security in Federal Buildings: Targeting Funds to Real Risks and Eliminating Unnecessary Security Obstacles
Primary:	The Honorable Eleanor Holmes Norton
Committee:	TRANSPORTATION (HOUSE)

Question: According to DOT testimony, the Secretary of DOT is solely responsible, without limitation, for protecting DOT headquarters and he has this authority through a delegation of authority. Is this standard practice to delegate your authority?

Response: Since FPS transferred from the General Services Administration (GSA) to the Department of Homeland Security (DHS) in 2003, it is not standard practice for FPS to delegate its security authority to other departments and agencies. However, prior to joining DHS, security delegations of authority had been issued. With some exceptions for those agencies that have full-time law enforcement and security forces on-site, when the delegations of authority issued by GSA are up for renewal, FPS will not renew those delegations. It should also be noted that some agencies have relinquished their delegations and requested that FPS provide services.

Question#:	8
Topic:	directives
Hearing:	Risk-based Security in Federal Buildings: Targeting Funds to Real Risks and Eliminating Unnecessary Security Obstacles
Primary:	The Honorable Eleanor Holmes Norton
Committee:	TRANSPORTATION (HOUSE)

Question: Within 30 days, please provide the Subcommittee with the directives that all agencies must use as guidelines for their protective services.

Response: Please see attachment. This is an FOUO document and not suitable for inclusion in a public hearing record. Please use for Committee staff access only.

Question#:	9
Topic:	plan
Hearing:	Risk-based Security in Federal Buildings: Targeting Funds to Real Risks and Eliminating Unnecessary Security Obstacles
Primary:	The Honorable Eleanor Holmes Norton
Committee:	TRANSPORTATION (HOUSE)

Question: Within 30 days, please provide to the Subcommittee information on a plan submitted to Immigration and Customs Enforcement to standardize the Federal Protective Service.

Response: NPPD in concert with FPS is working on the path forward and will engage the Committee when the appropriate path forward is determined.