EXAMINING SECURITY AT FEDERAL FACILITIES: ARE ATLANTA'S FEDERAL EMPLOYEES AT RISK?

HEARING

BEFORE THE

COMMITTEE ON GOVERNMENT REFORM

HOUSE OF REPRESENTATIVES

ONE HUNDRED SEVENTH CONGRESS

SECOND SESSION

APRIL 30, 2002

Serial No. 107–82

Printed for the use of the Committee on Government Reform

Available via the World Wide Web: http://www.gpo.gov/congress/house
http://www.house.gov/reform

U.S. GOVERNMENT PRINTING OFFICE

80–883 PDF WASHINGTON : 2001

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

COMMITTEE ON GOVERNMENT REFORM

DAN BURTON, Indiana, *Chairman*

BENJAMIN A. GILMAN, New York
CONSTANCE A. MORELLA, Maryland
CHRISTOPHER SHAYS, Connecticut
ILEANA ROS-LEHTINEN, Florida
JOHN M. MCHUGH, New York
STEPHEN HORN, California
JOHN L. MICA, Florida
THOMAS M. DAVIS, Virginia
MARK E. SOUDER, Indiana
STEVEN C. LATOURETTE, Ohio
BOB BARR, Georgia
DAN MILLER, Florida
DOUG OSE, California
RON LEWIS, Kentucky
JO ANN DAVIS, Virginia
TODD RUSSELL PLATTS, Pennsylvania
DAVE WELDON, Florida
CHRIS CANNON, Utah
ADAM H. PUTNAM, Florida
C.L. "BUTCH" OTTER, Idaho
EDWARD L. SCHROCK, Virginia
JOHN J. DUNCAN, JR., Tennessee
JOHN SULLIVAN, Oklahoma

HENRY A. WAXMAN, California
TOM LANTOS, California
MAJOR R. OWENS, New York
EDOLPHUS TOWNS, New York
PAUL E. KANJORSKI, Pennsylvania
PATSY T. MINK, Hawaii
CAROLYN B. MALONEY, New York
ELEANOR HOLMES NORTON, Washington, DC
ELIJAH E. CUMMINGS, Maryland
DENNIS J. KUCINICH, Ohio
ROD R. BLAGOJEVICH, Illinois
DANNY K. DAVIS, Illinois
JOHN F. TIERNEY, Massachusetts
JIM TURNER, Texas
THOMAS H. ALLEN, Maine
JANICE D. SCHAKOWSKY, Illinois
WM. LACY CLAY, Missouri
DIANE E. WATSON, California
STEPHEN F. LYNCH, Massachusetts

BERNARD SANDERS, Vermont
(Independent)

KEVIN BINGER, *Staff Director*
DANIEL R. MOLL, *Deputy Staff Director*
JAMES C. WILSON, *Chief Counsel*
ROBERT A. BRIGGS, *Chief Clerk*
PHIL SCHILIRO, *Minority Staff Director*

CONTENTS

EXAMINING SECURITY AT FEDERAL FACILITIES: ARE ATLANTA'S FEDERAL EMPLOYEES AT RISK?

TUESDAY, APRIL 30, 2002

HOUSE OF REPRESENTATIVES,
COMMITTEE ON GOVERNMENT REFORM,
Atlanta, GA.

The subcommittee met, pursuant to notice, at 10:30 a.m., in the Summit Building, 401 West Peachtree Street, Atlanta, GA, Hon. Bob Barr (vice chairman of the committee) presiding.

Present: Representatives Barr and LaTourette.

Staff present: Daniel R. Moll, deputy staff director; Robert A. Briggs, chief clerk; Susan Mosychuk, counsel; and David Rapallo, minority counsel.

Mr. BARR. I hereby convene this hearing of the Committee on Government Reform of the U.S. House of Representatives open. The focus of the hearing will be to examine security at Federal facilities, are Atlanta's Federal employees at risk.

The events of September 11, 2001 have focused our attention on a frightening reality. Even our most sacred institutions are vulnerable to attack. Terrorists do not engage in conventional warfare.

While terrorists may attack or threaten our military, the most tempting terrorist targets of choice are innocent and unsuspecting civilians. They use fear as a weapon, and will go to whatever extreme to heighten the shock effect.

Terrorists also seek to exploit environments that are a normal part of our daily routine. They aim to take out large numbers of victims to generate high media attention, and engender mass panic and public anxiety. What better targets than high profile landmarks and government institutions.

Government buildings are among the most visible institutions in our society by design, and selecting them for attack serves a very distinct purpose. When they attack these institutions the terrorists not only kill, maim, and destroy, but also instill fear that our government is unable to protect us. When terrorists attack, they are always trying to catch their victims in situations where they would otherwise feel safe. How safe are we in our Federal buildings?

The September 11th terrorist attacks in New York and at the Pentagon prompted immediate security crackdowns in Washington, DC, including the closing of streets, bolstering the security presence at Federal buildings, and curtailing visitor access to government compounds and buildings. Securing Federal buildings in the Nation's Capitol is clearly of vital importance. However, we must

not overlook the quality and effectiveness of security in all buildings and facilities occupied by Federal employees and visitors in every major city and across the Nation.

Congress and the Federal Government had the opportunity to lead by example working with the District of Columbia, local business leaders, and concerned citizens to meet security needs without necessarily impeding the city's or the government's ability to go about its daily business in the Capitol.

Despite the workable security measures deployed at Federal facilities in Washington, DC, many local Federal agencies have not addressed, or remain unable to address security needs in the aftermath of last year's terrorist attacks. Many media outlets reported that security procedures at Federal agencies varied tremendously in both process and effect throughout the country. Inconsistent and vague security procedures at our Federal facilities leave thousands of Federal employees, visitors, and constituents highly vulnerable and at risk. The extent to which our government buildings are vulnerable to attack should concern not only the Federal employees of these buildings, but every family member of these employees, any member of the general public visiting these buildings, and any individual or company that conducts business with an agency housed in one of these buildings. In other words, this concerns every member of our community.

Building security is not just about securing the physical structure itself; it is about protecting the lives and livelihood of everyone and everything in these buildings.

Consider for a moment the repercussions of a terrorist attack at the IRS service center here in Atlanta. The building which you can see a picture of here houses 3,000 occupants and is the main processing center for the entire Southeast Region of the United States. The human toll would be staggering, and the financial impact devastating.

Or consider the repercussions of a terrorist attack at the Sam Nunn Federal Building. Look at the sheer numbers of employees and the variety and importance of the government agencies that would be directly affected.

Today representatives from the General Accounting Office, Office of Special Investigations [OSI], will provide testimony on the results of a recently completed investigation. At the request of this committee the investigators tested security measures at five Federal office buildings in the Atlanta area, which has one of the largest Federal presences outside of Washington, DC.

Acting in an undercover capacity investigators were able to gain unauthorized access to every secured government building they attempted to penetrate. Not only were the investigators able to gain unauthorized access to these buildings, they gained access which allowed them unfettered admission to any areas of the buildings day or night.

The ease whereby the investigators were successful is shocking. A simple pretext was concocted and easily carried out, allowing agents to obtain building passes. In fact, they were able to obtain passes which denote the bearer as being authorized to carry firearms. This building pass allowed them to move freely about, and extensively bypassing magnetometers and x-ray machines. They

even obtained an after-hours access code allowing them to enter the facilities after security personnel had gone home.

By employing a few simple tactics and off-the-shelf technology investigators thwarted the security in such a manner that weapons, explosives, nuclear, chemical, or biological agents, listening devices, and other life-threatening or hazardous materials could have easily been carried into and left throughout these Federal buildings. They were given in effect the keys to the kingdom. In the words of the investigators, they owned those buildings.

At a time when Federal facilities are operating under the highest level of security, these undercover investigators were able to freely enter the buildings without proper identification or authority carrying packages which had not been scanned or inspected.

The problem is not isolated to the Atlanta area alone. The Department of State in Washington, DC, recently had to overhaul its security operations following a string of serious breaches compromising classified information.

It had been an open secret that security was lax at State. In fact, in late 1998 an unidentified man in a brown tweed jacket entered then Secretary of State Albright's executive suite and carried out unchallenged a pile of classified documents. He was never seen again.

We no longer live in an environment in which we can afford such a casual attitude toward security and safety. All principal personnel must stress the importance of security, and combat perceived weaknesses in the security culture, and proper measures must be demanded and enforced.

Beyond that, there are specific areas in which we can focus with regard to security personnel, training, and equipment. Following numerous security reviews, inspections, and reports one major area for reform at the State Department was tightening controls of the State Department building passes. At the time there were 33,000 State Department passes with 2,000 per year completely lost. Diplomats kept their passes even when stationed overseas, making those passes prime targets for theft or misuse.

Given the potential threat, State Department began a process of redoing all building passes, deactivating those of former employees, and making the process of obtaining them much tougher.

Implementing security procedures with the aim of thwarting any and every conceivable infiltration would be impractical. To do that would make daily operations of our government agencies impossible. However, we can, and should, and must make buildings both safe and accessible by consistently following guidelines, deploying appropriate technology, and employing basic common sense.

We must take a rational approach to security to ensure safety concerns are addressed in a manner that does not make things worse. We cannot allow terrorism to destroy our sense of community or the ability of the institutions that run our government to serve us.

Understanding the nature of terrorist attacks and how terrorists organizations operate helps us prepare and prevent future attacks. We can regain control and eliminate fear by taking proactive steps to avoid falling victim.

I thank the witnesses that will be appearing here today, and look forward to working with them and others on a subsequent legislative remedy to provide an oversight remedy to provide security procedures at our Federal installations.

While the results of this current investigation are frightening, we hope the steps taken in response will be reassuring in both effect and perception.

[The prepared statement of Hon. Bob Barr follows:]

Opening Statement
The Honorable Bob Barr, Vice Chairman
Committee on Government Reform
Hearing on: "Examining Security at Federal Facilities: Are Atlanta's Federal Employees At Risk?"

The events of September 11th have focused our attention on a frightening reality: even our most sacred institutions are vulnerable to attack.

Terrorists do not to engage in conventional warfare.

While terrorists may attack or threaten our military, the most tempting terrorist targets of choice are innocent and unsuspecting civilians. They use fear as a weapon, and will go to whatever extreme to heighten the shock effect.

Terrorists also seek to exploit environments that are a normal part of our daily routine. They aim to take out large numbers of victims to generate high media attention and engender mass panic and public anxiety. What better target than high-profile landmarks and government institutions? Government buildings are among the most visible institutions in our society, and selecting them for attack serves a distinct purpose. When they attack these institutions, the terrorists not only kill, maim and destroy, but also instill fear our government is unable to protect us.

When terrorists attack, they are always trying to catch their victims in situations where they would otherwise feel safe.

How safe are we in our federal buildings?

The September 11th terrorist attacks in New York and at the Pentagon prompted immediate security crackdowns in

Washington, D.C.; including the closing of streets, bolstering the security presence at federal buildings, and curtailing visitor access to government compounds and buildings.

Securing federal buildings in the nation's capitol is clearly of vital importance. However, we must not overlook the quality and effectiveness of security in *all* buildings and facilities occupied by federal employees and visitors, in every major city and across the nation.

Congress and the federal government had the opportunity to lead by example, working with the District of Columbia, local business leaders and concerned citizens, to meet security needs without unnecessarily impeding the city's ability to go about its daily business.

Despite the workable security measures deployed at federal facilities in Washington, D.C, many *local* federal agencies have not addressed, or remain unable to address, security needs in the aftermath of the terrorist attacks. Many media outlets reported that security procedures at federal agencies vary tremendously -- in both process and effect -- throughout the country.

Inconsistent and vague security procedures at our federal facilities leave thousands of federal employees, visitors and constituents highly vulnerable and at risk.

The extent to which our government buildings are vulnerable to attack should concern not only the federal employees of these buildings, but every family member of these employees, any member of the general public visiting these buildings, and any individual or company that conducts business with an agency housed in one of these buildings - - in other words, this concerns every member of this community.

Building security is not about just securing the physical structure itself – it is about protecting the lives and livelihood of everyone and everything in these buildings.

Consider for a moment the repercussions of a terrorist attack at the IRS Service Center here in Atlanta. The building houses 3,000 occupants and is the main processing center for the entire southeast region of the United States. The human toll would be staggering, and the financial impact devastating.

Or consider the repercussions of a terrorist attack at the Sam Nunn Federal Building. Look at the sheer number of employees and the government agencies affected.

Today, representatives from GAO's (the General Accounting Office) Office of Special Investigations will provide testimony on the results of a recently completed investigation. At the request of the Committee, the investigators tested security measures at five federal office buildings in the Atlanta area, which has one of the largest federal presences outside Washington.

Acting in an undercover capacity, investigators were able to gain unauthorized access to *every* secure government building they attempted to penetrate.

Not only were the investigators able to gain unauthorized access to these buildings, they gained access which allowed them unfettered admission to *any* area at all the buildings, *anytime*- day or night.

The ease whereby the investigators were successful, is shocking. A simple pretext was concocted, and easily carried out; allowing agents to obtain building passes. In fact, they were able to obtain passes which denote the bearer as being authorized to carry firearms. This building pass allowed them to move about freely and extensively, bypassing magnetometers and X-ray machines.

They even obtained an after-hours access code, allowing them to enter the facilities after security personnel had gone home.

By employing a few simple tactics, investigators thwarted the security in such a manner that weapons, explosives, nuclear, chemical, or biological agents, listening devices and other life-threatening or hazardous material, could have been carried into and throughout these buildings.

They were given, in effect, the keys to the kingdom. In the words of the investigators: they "owned" those buildings.

At a time when federal facilities are operating under the highest level of security, these undercover investigators were able to freely enter the buildings, without proper identification or authority, carrying packages which had not been scanned or inspected.

This problem is not isolated to the Atlanta area, alone. The Department of State in Washington, D.C. recently had to overhaul its security operations following a string of serious breaches compromising classified information. It had been an open secret that security was lax at State. In fact, in late 1998, an unidentified man in a brown tweed jacket entered then-Secretary of State Albright's executive suite and walked out, unchallenged, with a pile of classified documents. He was never seen again.

We no longer live in an environment in which we can afford such a casual attitude towards security and safety. All principal personnel must stress the importance of security and combat perceived weaknesses in the security culture; and proper measures must be demanded and enforced.

Beyond that, there are specific areas on which we can focus with regard to security personnel, training and equipment.

Following numerous security reviews, inspections and reports, one major area for reform at the State Department was tightening controls of State Department building passes. At the time there were 33,000 State Department building passes, with 2,000 per year lost. Diplomats kept their passes even when stationed overseas, making those passes prime targets for theft or misuse. Given the potential threat, the department began a process of redoing all building passes, de-activating those of former employees, and making the process of obtaining them much tougher.

Implementing security procedures with the aim of thwarting any and every conceivable infiltration would be impractical. To do that would make daily operations of our government agencies impossible. But, we can make public buildings both safe and accessible by consistently following guidelines, deploying appropriate technology, and employing some basic common sense. We must take a rational approach to security, to ensure safety concerns are addressed in a manner that does not make things worse. We cannot allow terrorism to destroy our sense of community or the ability of the institutions that run our government to serve us.

Understanding the nature of terrorist attacks and how terrorist organizations operate helps us prepare and prevent for such an attack. We can regain control and eliminate fear by taking proactive steps to avoid falling victim.

I thank the witnesses for appearing here today, and look forward to working with you all on a subsequent legislative remedy to improve security procedures at our federal installations.

While the results of this investigation are frightening, we hope the steps taken in response will be reassuring.

Mr. BARR. I would like to now turn to my colleague from the State of Ohio, a senior member of our Government Reform Committee, Steve LaTourette.

Mr. LATOURETTE. Thank you very much, Chairman Barr. And first of all thank you for inviting me to Atlanta. And second I want to commend Congressman Barr for the leadership that you and the chairman of our full committee, Dan Burton of Indiana, have demonstrated in dealing with the security of the Federal buildings, this particular issue, and you in particular because of your concern for the men and women that work in the buildings in Atlanta, Ga.

As you correctly point out in your opening remarks the security of the Federal work force and those who visit the Federal buildings in the United States is of vital concern to the government. In 1995 one of the shocking revelations that came to our attention after the bombing of the Murrah Federal Building in Oklahoma City was that there was one contract guard assigned to three different buildings on that occasion, and clearly security was not where we needed to be in 1995. I think many of us hoped that in the years between 1995 and certainly 2002 improvements have been made.

The report that we are here to talk about today is disturbing. Although the agents that we will hear from are certainly skilled at what they do, the ability to completely breach the buildings in Atlanta, GA I think is incomprehensible in the wake of September 11th.

Hopefully this hearing and other hearings like it will help assist not only the agencies in charge of the security, but also the Congress and the administration reach some conclusions that can make these buildings safer.

One of the other happy tasks that I have in the Congress is chairing the Public Buildings, Economic Development, and Emergency Management Subcommittee of Transportation and Infrastructure that has concurrent jurisdiction over some of the issues that we are going to be talking about today, and the good news is that legislation relative to the Federal Protective Service is in fact moving through that committee, and one of the alarming notes I would say is that we appear to be going backward. When we talked to Steve Perry, the administrator of the General Services Administration, the goal was to beef up the Federal Protective Service work force from 600 full-time employees to 900, and what we have seen instead according to Mr. Perry is that they have gone down to 450, and the reason being—and we must bear some of that responsibility—is that there is about a $10,000 starting salary differential between what someone for FPS can make and what someone can make working for the Capitol Hill police department. So that is an example of some of the things that we are going to have to take a look at in the Congress.

The other thing that the hearings revealed on this particular issue is that the training received by the contract guard authorities utilized by GSA do not receive equivalent training to those who are employed as police officers in my home State of Ohio or here in the State of Georgia, and training is something that we also have to emphasize.

And last, I am not a big believer in gotcha anything, but I did read the report, I read the recommendations following the briefing

of the GAO officers, and one of the recommendations was that there be at least three people stationed by the magnetometers, and during our break I went outside to engage in one of the few vices I am allowed, and that is to have a cigarette, and I came back in through the building and there were only two stationed at the magnetometer that I entered, and I am also today in possession of two visitors passes permitting me access to this building, and it seems to me that we can address that during the hearing as well to determine how that could be.

I thank you very much.

Mr. BARR. Is that in case you lose one?

Mr. LATOURETTE. I do not know if it is in case I lose one, or in case I have another visitor I want to bring with me.

I appreciate very much the opportunity to be here today, and I thank you again for your leadership.

Mr. BARR. Thank you very much.

For those unfamiliar with hearings conducted by the Government Reform Committee, basically what we will do now is we will swear in the five witnesses, and we will hear from each one of them if in fact each one of them wishes to make an opening statement for the record. If there is any additional material that any of our witnesses seeks to be made a part of the record either in more extensive opening statement or additional material that might come to light, or be relevant based on subsequent questions, the record will remain open for 10 days for the submission of any additional material.

Following the opening statements of witnesses, Mr. LaTourette and I will ask questions. If counsel has any additional questions, she will ask questions as well. And then we will conclude the hearing.

At this time if the five witnesses would stand, please, to be sworn. If you would raise your right hands.

[Witnesses sworn.]

Mr. BARR. Let the record reflect that all witnesses responded in the affirmative. Thank you, and please be seated.

We have five very distinguished witnesses here today, all of whom have the same goal in mind that we on this committee do, and that is to provide the very best security for not just the Federal buildings and Federal employees and their families, but all who visit, come in contact with, or have an interest in our Federal Government, and we appreciate each one of them being with us today to assist us in our oversight responsibilities to ensure this vital function of our Federal Government is carried out, and to hear from them not only with regard to what steps they have and believe ought to be taken, but ways in which we in the Congress might help. As Mr. LaTourette mentioned, we in the Congress have a responsibility to make sure that the laws reflect the needs of our Federal agencies and our Federal officials, and also that the funds necessary to carry out those functions are made available. So this is very much a team effort, and we appreciate again the witnesses being with us today.

The witnesses that we will hear from today—I believe there is a witness list available in the back of the room—we will hear from in the following order.

Mr. Ronald Malfi, the Acting Managing Director, Office of Special Investigations, General Accounting Office. He has extensive background which he is certainly free to go into to establish his bona fides in the Secret Service.

Also then testifying second will be Mr. Patrick Sullivan, the Assistant Director, Office of Special Investigations for the General Accounting Office, also with extensive background in law enforcement and particularly with the Secret Service; and finally testifying on behalf of GAO will be Mr. John Cooney, Special Agent, Office of Special Investigations, General Accounting Office, with a similar and very extensive and distinguished background in Federal law enforcement.

We will then hear from Mr. Wendell Shingler, the Assistant Commissioner of the Office of Federal Protective Service [FPS], of the General Services Administration. The General Services Administration is generally known as the government's landlord. It is the responsibility of GSA to maintain thousands of Federal buildings all across the country, including many of those here in the Atlanta area.

And finally testifying will be Ms. Sabina Sims, the Director of the Office of Federal Protective Service for GSA Region 4 which includes as its center Atlanta, GA.

With that introduction, Mr. Malfi, the floor is yours to make an opening statement, and if you would basically lay out the parameters of why your agency got involved in this investigation and how you carried it out.

STATEMENTS OF RONALD MALFI, ACTING MANAGING DIRECTOR, OFFICE OF SPECIAL INVESTIGATION, GENERAL ACCOUNTING OFFICE; JOHN COONEY, SPECIAL AGENT, OFFICE OF SPECIAL INVESTIGATIONS, GENERAL ACCOUNTING OFFICE; PATRICK F. SULLIVAN, ASSISTANT DIRECTOR, OFFICE OF SPECIAL INVESTIGATIONS, GENERAL ACCOUNTING OFFICE; WENDELL C. SHINGLER, ASSISTANT COMMISSIONER, OFFICE OF FEDERAL PROTECTIVE SERVICE, GENERAL SERVICES ADMINISTRATION; AND SABINA SIMS, DIRECTOR, OFFICE OF FEDERAL PROTECTIVE SERVICE, GSA REGION 4

Mr. MALFI. Thank you. Mr. Chairman, members of the committee. We are here today to discuss the results of our tests of security measures at Federal office buildings in the Atlanta, GA area. Specifically you asked that special agents of the Office of Special Investigations acting in an undercover capacity attempt to gain unauthorized access to secure facilities in such a manner that weapons, explosives, chemical/biological agents, listening devices, or that hazardous materials could have been brought into these facilities.

During February and March 2002 our agents breached the security at four of the Federal office buildings that we tested in the Atlanta area by entering these buildings without proper authority, carrying a briefcase or package, and bypassing the magnetometers and x-ray machines. They were able to move freely and extensively throughout these facilities during both day and evening hours, and were not challenged by anyone. Our undercover agents could have carried in weapons, listening devices, explosives, chemical/biological agents, or other such items.

All buildings required screening of visitors and valises, for example briefcases and baggage, which included the use of magnetometers and x-ray machines at security checkpoints.

The buildings required the wearing of either a blue pass or a yellow pass for identification of employees working in these buildings, which allowed them to bypass the magnetometers and x-ray machines.

The blue pass could also have an additional feature added to it that would denote the bearer as being authorized to carry a firearm. All passes included photo identification, and had holograms on them, but were worn inside plastic pockets that could partially obscure the hologram as well as the bearer's photograph.

Mr. BARR. Excuse me, Mr. Malfi. Do you have a couple of those badges we could look at while you are testifying?

Mr. MALFI. Yes, I do.

One of the badges that you are going to be getting, sir, is the genuine, and one is the counterfeit badge. The genuine badge has the holograms that are easily seen when they are reflected off the light.

Mr. BARR. This one?

Mr. MALFI. That is correct. The other is a counterfeit badge.

Mr. BARR. And they were put in these plastic pouches?

Mr. MALFI. That is how they were handed out. When the building passes were given out, these plastic pouches came with the passes. And you will note one side of the plastic is clear, the other side is opaque, and we put the photograph, the building pass with the photograph and the hologram in the opaque side to obscure it.

Mr. BARR. Without going into—and I do not want you to disclose particularly sensitive investigative techniques here—would you describe what a pretext is?

Mr. MALFI. Basically a pretext is a ruse that we concocted in order to allow ourselves to get into the building and to meet with GSA people who were issuing the passes.

Mr. BARR. A story?

Mr. MALFI. It is a story, a fabricated story to give the people a reason as to why we needed these passes.

Mr. BARR. Was there anything particularly complex about that story? Could anybody have made something up?

Mr. MALFI. That is correct. We used one ruse; we could have used one of many ruses to get into the building in order to obtain a building pass.

Mr. BARR. Thank you.

Mr. MALFI. You are welcome.

I am going to go into how we exactly breached the security of these buildings.

In early March using a pretext for gaining access, an agent who had no building pass entered one of the buildings carrying a briefcase, bypassing the magnetometer and the x-ray machines. He met with the General Services Administration employee responsible for issuing building passes, and obtained a yellow building pass and an after-hours access code for that building.

The next day the same agent entered another building carrying a briefcase. He showed his yellow pass and stated that he wanted to obtain a blue pass for that building, and bypassed the

magnetometers and the x-ray machines based on the strength of the yellow pass.

Mr. BARR. Do you have that yellow pass, please?

Mr. MALFI. Yes.

He then met with the GSA contract employee responsible for issuing building passes, and based solely on the strength of having a yellow pass obtained a blue building pass and an after-hours access code to two of the subject buildings.

In addition, this agent was able to obtain a second feature on the blue building pass that identified him as a law enforcement officer and permitted him to carry a firearm in those buildings.

Finally, through the use of another pretext the same agent obtained——

Mr. BARR. Excuse me. There is a specific designation on the badge that the folks at the building would know authorized the bearer to carry a firearm in the building?

Mr. MALFI. That is correct. It is a little round insignia that would notify the marshals basically that the bearer had the right to carry a firearm.

Finally, through the use of another pretext the same agent obtained the security guard's after-hours access code for one of the buildings.

Mr. BARR. This would be a security code that was designated specifically to that particular person?

Mr. MALFI. That is correct.

Mr. BARR. And he gave it to the undercover agent, yourself, or one of your colleagues——

Mr. MALFI. That is correct.

Mr. BARR [continuing]. So that they could get into the building after hours?

Mr. MALFI. Based again on some social engineering we had an access code that allowed us entry to the building at night.

Mr. BARR. What do you mean social engineering?

Mr. MALFI. Basically conning the security guard into having him reveal his access code. The importance to that would have been that if anything would have occurred we could have used that access code to gain entry into the buildings after hours. If something—we could have put explosives in the building, and basically if they would have went back and checked who entered in they never would have even been able to check it to our false identification. They would have wound up going back to the guard as one of the people that gained entry into that building that night.

Then after we received the original passes we counterfeited both the yellow and blue building passes using commercially available software, inserting in them the fictitious names used by our undercover agents and their photographs in preparation for an attempt as a group to breach the security of these facilities.

Mr. BARR. Excuse me. In other words, the software that was used to create the false badges is available to anybody on the open market? It was not something that was uniquely available to yourselves as law enforcement officials and investigators?

Mr. MALFI. That is correct. Everything that we did and we used was available to the public. We did not use any of our inside technology in order to enhance this operation. We wanted to make it

that anyone basically without being involved in the law enforcement community could have accomplished what we did.

The counterfeit passes contained printed holograms on them, not actual holograms. Had anyone made a physical inspection of the counterfeit passes they should have been able to detect them as being bogus.

Mr. BARR. In other words, the hologram that is available if you look at it?

Mr. MALFI. That is correct. On the counterfeit ones we just printed a duplicate of the hologram which did not perform the function that a hologram does. It does not change shades when it is exposed to the light or moved; it is flat.

Mr. BARR. And that is obvious to us, and it would have been obvious had one of the guards checked it, just physically looked at it for a moment?

Mr. MALFI. That is correct.

Mr. BARR. But that did not happen?

Mr. MALFI. That is correct.

Later in March other agents using the counterfeit yellow and blue building passes entered three of the buildings bypassing the magnetometers and x-ray machines. One of these agents carried a briefcase. The same agents also successfully entered these same buildings in the evening utilizing the access codes that they previously acquired.

An agent using a counterfeit yellow building pass met with the GSA contract employee responsible for issuing building passes for the two buildings. Based on the strength of the counterfeit yellow pass and a fictitious request form the agent was issued a genuine blue building pass and an access code for the evening entry after security check points were closed.

Additionally, one agent wore another agent's legitimate blue pass into one of the buildings, crossed over into another building through a tunnel, and was never challenged.

Mr. BARR. Is there a physical similarity between the person who utilized that badge and the picture on the badge?

Mr. MALFI. Actually I used Agent Cooney's picture identification to gain access into the buildings.

Mr. BARR. I will not ask which one of you was insulted, but in other words you used the badge of somebody that does not look very much like you at all, and you were not challenged?

Mr. MALFI. That is correct.

Two agents then drove to another Federal facility, and based on the strength of a legitimate yellow pass and a counterfeit yellow pass and a pretext gained admittance to that building bypassing the magnetometer and x-ray machines.

Finally, after we completed our test of the security for these buildings we met with officials from the U.S. attorney's office, the U.S. Marshal Service, GSA, and the Federal Protective Service, and briefed them on the results of the security tests, identifying the weaknesses we found.

Mr. BARR. This was immediately following the conclusion of your investigation?

Mr. MALFI. That is correct. Actually the day that I wore the pass was the day of the meeting, so we were finished. As soon as we fin-

ished the actual last function of the operation we immediately had a meeting with these individuals and advised them of the weaknesses that we found.

Subsequently, the Federal Protective Service issued a security bulletin which addressed weaknesses we identified.

In closing, I would like to add that last week GAO's chief technologist testified at a hearing before the Subcommittee on Technology and Procurement Policy, House Committee on Government Reform, concerning security technologies to protect Federal facilities. As part of that testimony it was acknowledged that effective security also entails having a well-trained staff that follows and enforces policies and procedures. It was noted that breaches in security resulting from human error are more likely to occur if personnel do not understand the risks and the policies that are put in place to mitigate them. Good training is essential to successfully implementing policies by ensuring that personnel exercise good judgment following security procedures.

Cited as an example was our previous work where we breached the security at 19 Federal agencies and two airports. This case further exemplifies this point. Further, the Federal Protective Service bulletin reinforces this point.

Mr. Chairman, that completes my prepared statement. We would be happy to respond to any questions you have, or members of the committee. Thank you.

[The prepared statement of Mr. Malfi follows:]

United States General Accounting Office

GAO

Testimony

Before the Committee on Government Reform, U.S. House of Representatives

For Release on Delivery
Expected at 10:00 a.m.
Tuesday, April 30, 2002

SECURITY BREACHES AT FEDERAL BUILDINGS IN ATLANTA, GEORGIA

Statement of Ronald Malfi, Acting Managing Director
Office of Special Investigations

GAO-02-668T

Mr. Chairman and Members of the Committee:

We are here today to discuss the results of our test of security measures at federal office buildings in the Atlanta, Georgia, area. Specifically, you asked that special agents of the Office of Special Investigations, acting in an undercover capacity, attempt to gain unauthorized access to secure facilities in such a manner that weapons, explosives, chemical/biological agents, listening devices, or other hazardous material could have been brought into these facilities.

During February and March of 2002, our agents breached the security at four of the federal office buildings that we tested in the Atlanta area by entering these buildings without proper authority, carrying a briefcase or package and bypassing the magnetometers and X-ray machines. They were able to move freely and extensively throughout these facilities during both day and evening hours and were not challenged by anyone. Our undercover agents could have carried in weapons, listening devices, explosives, chemical/biological agents, or other such items.

All buildings required screening of visitors and valises, for example, briefcases and baggage, which included the use of magnetometers and X-ray machines at security checkpoints. The buildings required the wearing of either a blue pass or a yellow pass for identification of employees working in these buildings, which allowed them to bypass the magnetometers and X-ray machines. The blue pass could also have an additional feature added to it that would denote the bearer as being authorized to carry firearms. All passes included photo identification and had holograms on them, but were worn inside plastic pockets that can partially obscure the hologram as well as the bearer's photograph.

How Security Was Breached

In early March, using a pretext for gaining access, an agent who had no building pass entered one of the buildings carrying a briefcase, bypassing the magnetometer and X-ray machines. He met with the General Service Administration (GSA) employee responsible for issuing building passes, and obtained a yellow building pass and an after-hours access code for that building.

The next day the same agent entered another building carrying a briefcase. He showed his yellow pass and stated that he wanted to obtain a blue pass for that building and bypassed the magnetometer and X-ray machines based on the strength of the yellow pass. He then met with a GSA contract employee responsible for issuing building passes and, based solely on the

strength of having a yellow pass, obtained a blue building pass and an after-hours access code for two of the subject buildings. In addition, this agent was able to obtain a second feature on the blue building pass that identified him as a law enforcement officer and permitted him to carry a firearm in those buildings.

Finally, through the use of another pretext, the same agent obtained a security guard's after-hours access code for one of the buildings. He successfully used the guard's access code and the access code given to him by the GSA employee to enter this building during the evening and was thereafter able to move freely about the building without being challenged.

We then counterfeited both the yellow and blue building passes, using commercially available software, inserting in them the fictitious names used by other undercover agents and their photographs in preparation for our attempt as a group to breach the security at these facilities. The counterfeit passes contained printed holograms, not actual holograms. Had anyone made a physical inspection of our counterfeited passes, they should have been detected as being bogus.

Later in March, other agents using counterfeit yellow and blue building passes entered three of the buildings bypassing the magnetometers and X-ray machines. One of these agents carried a briefcase. These same agents also successfully entered these same buildings in the evening utilizing the access codes that were previously acquired. An agent, using a counterfeit yellow building pass, met with the GSA contract employee responsible for issuing building passes for two of the buildings. Based on the strength of the counterfeit yellow pass and a fictitious request form, the agent was issued a blue building pass and an access code number for evening entry after the security checkpoints were closed. Additionally, one agent wore another agent's legitimate blue pass into one of the buildings, crossed over into another building through a tunnel, and was never challenged.

Two agents then drove to another federal facility and, based on the strength of a legitimate yellow pass, a counterfeit yellow pass, and a pretext, gained admittance to that building bypassing the magnetometer and X-ray machines.

Finally, after we completed our test of the security for these buildings, we met with officials from the U.S. Attorney's Office, U.S. Marshals Service, GSA, and Federal Protective Service and briefed them on the results of the

security tests, identifying the weaknesses found. Subsequently, the Federal Protective Service issued a security bulletin which addressed the weaknesses we identified.

In closing, I'd like to add that last week GAO's Chief Technologist testified at a hearing before the Subcommittee on Technology and Procurement Policy, House Committee on Government Reform, concerning security technologies to protect federal facilities.[1] As part of that testimony it was acknowledged that effective security also entails having a well-trained staff that follows and enforces policies and procedures. It was noted that breaches in security resulting from human error are more likely to occur if personnel do not understand the risks and the policies that are put in place to mitigate them. Good training is essential to successfully implementing policies by ensuring that personnel exercise good judgment in following security procedures. Cited as an example was our previous work where we breached the security at 19 federal agencies and 2 airports.[2] This case further exemplifies this point. Further, the Federal Protective Service bulletin reinforces this point.

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

[1] See *National Preparedness: Technology to Secure Federal Buildings*, U.S. GAO-02-481T (April 25, 2002).
[2] See *Breaches at Federal Buildings and Airports*, U.S. GAO/T-OSI-00-10 (May 25, 2000).

Mr. BARR. Thank you, Mr. Malfi.
Mr. Sullivan, do you have an opening statement?
Mr. SULLIVAN. No, sir, I do not have an opening statement.
Mr. BARR. Mr. Cooney?
Mr. COONEY. Also I have none.
Mr. BARR. You are both available to answer any questions?
Mr. COONEY. Yes, sir.
Mr. SULLIVAN. Yes, sir.
Mr. BARR. Mr. Shingler.
Mr. SHINGLER. Good morning, Mr. Chairman, members of the committee.

I am Wendell Shingler, Assistant Commissioner of the Federal Protective Service, General Services Administration [GSA]. Although I am relatively new to this position, I have 30 years of security experience in progressively more demanding positions within the Federal Government, most recently with the U.S. Marshal Service.

I look forward to the challenges that we face, as well as working with other Federal agencies in meeting their needs. I am pleased to appear before you today and provide information on the GSA's program to secure Federal buildings that it owns or leases, and the methodology that we use to assess potential vulnerabilities to these facilities.

GSA's Federal Protective Service [FPS] provides law enforcement and security to over 8,000 owned and leased buildings, and approximately 1 million Federal employees and visitors to these facilities on a daily basis.

We are comprised of police officers, criminal investigators, physical security specialists, and rely on the use of nearly 7,000 contract guards to supplement our needs.

With the terrorist attacks of September 11th there is one clear message: that there is no security silver bullet. Security is a dynamic and ever-changing discipline. GSA's Federal Protective Service strives to provide the safest environment for the Federal agencies we house and the American public that visit these Federal buildings. The threat and our response to it changes daily.

The dedicated men and women of the Federal Protective Service welcome that challenge, and are constantly striving to improve our services and reduce potential threats to our buildings. Our primary goal is to make everyone feel safe when entering GSA-controlled buildings.

Since there is no one-size-fits all in security to achieve this goal, each of our facilities receives an individual building security assessment. The building security assessment program is designed to determine the specific security measures needed to eliminate or reduce threats directly associated with each individual building. Tailored security measures, countermeasures are then recommended based on reducing or eliminating determined vulnerabilities and threats at buildings.

In addition, we are now working with the FBI, CIA, State and local law enforcement agencies in sharing of intelligence information that enables us to better assess the credibility of those threats.

In addition to physical countermeasures such as guards, physical barriers, alarms, cameras, x-ray machines, and magnetometers we

also provide law enforcement services. These services include responding to calls, arrests, and when necessary conducting investigations.

On a national level we accomplish this challenging and very important job of protecting GSA-controlled facilities with a small but dedicated uniformed staff. To augment our Civil Service force, we rely on 7,000 contract guards nationwide.

Here in GSA's Southeast Sunbelt Region we have 1,327 buildings of which 143 are Level 4, our highest security level. To protect these facilities we supplement our law enforcement personnel with 960 armed contract guards.

The only acceptable minimum security level for all of these facilities nationwide is that which provides a safe and secure environment for GSA co-workers, customers, and visitors. This is the driving force behind our FPS mission, to permit Federal agencies and members of the public to conduct their business without fear of violence, crime, or disorder.

I know I face many challenges in my new position, and I am certain that the Federal Protective Service and I are ready to take them on.

This concludes my prepared statement, Mr. Chairman, and we are prepared to answer any of your questions.

[The prepared statement of Mr. Shingler follows:]

STATEMENT OF

WENDELL C. SHINGLER

ASSISTANT COMMISSIONER

OFFICE OF FEDERAL PROTECTIVE SERVICE

PUBLIC BUILDINGS SERVICE

U.S. GENERAL SERVICES ADMINISTRATION

BEFORE THE

COMMITTEE ON GOVERNMENT REFORM

UNITED STATES HOUSE OF REPRESENTATIVES

April 30, 2002

Good morning Mr. Chairman, and members of the Subcommittee. I am Wendell Shingler, Assistant Commissioner of the Federal Protective Service. Although I'm relatively new to the position, I have 30 years of security experience in progressively more demanding positions within the Federal government, most recently with the U.S. Marshals Service. I look forward to the challenges that we face as well as working with other Federal agencies in meeting their needs. I am pleased to appear before you today to provide information on the General Services Administration's program to secure the federal buildings that it owns or leases and the methodology we use to assess potential vulnerabilities to these facilities.

GSA's Federal Protective Service provides law enforcement and security to over 8,000 owned and leased buildings and approximately one million federal employees and visitors to these facilities on a daily basis. We are comprised of police officers, criminal investigators, physical security specialists and rely on the use of nearly 7,000 contract guards to supplement our needs.

With the terrorists attacks of September 11th there is one clear message-- ***there is no security silver bullet***. Security is a dynamic and ever changing discipline. GSA's Federal Protective Service strives to provide the safest environment for the Federal agencies we house and the American public that visit Federal buildings. The threat and our response to it change daily. The dedicated men and women of the Federal Protective Service welcome that challenge and are constantly striving to improve our services and reduce potential threats to our buildings.

Our primary goal is to make everyone feel safe when entering a GSA-controlled building. Since there is no "**one size fits all**" in security to achieve this goal, each of our facilities receives an individual Building Security Assessment. The Building Security Assessment program is designed to determine the specific security measures needed to eliminate or reduce threats directly associated with each individual building.

Tailored security countermeasures are then recommended based on reducing or eliminating determined vulnerabilities and threats at that building. In addition, we are now working with the FBI, CIA and State and local law enforcement agencies in the sharing of intelligence information that enables us to better assess the credibility of threats.

In addition to physical countermeasures such as guards, physical barriers, alarms, cameras, x-ray machines and magnetometers, we also provide all necessary law enforcement services. These services include responding to calls, arrests when necessary and conducting investigations.

On a national level we accomplish this challenging and very important job of protecting GSA-controlled facilities with a small but dedicated force of 512 uniformed personnel. To augment our civil service force we rely on some 7,000 contract security guards nationwide. Here in GSA's Southeast Sunbelt Region, we have 1,327 buildings of which 143 are Level 4 facilities, the highest security level. To protect these facilities we are staffed with 53 law enforcement personnel and 960 armed contract guards.

The only acceptable minimum-security level for all of our facilities nationwide is that which provides for a safe and secure environment for our GSA co-workers, customers and visitors. This is the driving force behind our FPS mission to permit Federal agencies and members of the public to conduct their business without fear of violence, crime or disorder. I know I face many challenges in my new position and I'm certain that the Federal Protective Service and I are ready to take them on.

This concludes my prepared statement Mr. Chairman. We will be pleased to answer any questions you or the other members of the Committee may have on this matter.

Mr. BARR. Thank you, Mr. Shingler.

Ms. Sims, please.

Ms. SIMS. I have nothing further to add, but I would be more than happy to answer any specific questions that you have for me.

Mr. BARR. OK. Maybe you could briefly for the benefit of the audience and the listening public who are very concerned about this just very briefly describe the FPS or the Federal Protective Service and its function, and how it interfaces with GSA.

Ms. SIMS. The Federal Protective Service is the law enforcement and security arm of the U.S. General Services Administration. I am 1 of 11 FPS regional directors around this country, and I am the Director of the Southeast Sunbelt Region. I have approximately 1,300 facilities around eight States in this region.

Mr. BARR. OK. Thank you.

I have a couple of preliminary questions, and then I would like to turn to my colleague Mr. LaTourette, then I may have some more, and he may as well.

Back in 1993 the World Trade Center was bombed in the garage. Two years later the Murrah Federal Building in Oklahoma City was bombed and crumbled with tremendous loss of life, and of course on September 11th of last year our Nation suffered the most serious terrorist attacks ever perpetrated against us in our homeland or anywhere.

After each one of those I would presume that our government took a look at security procedures, not just at Federal buildings, but particularly at Federal buildings, and took steps to address those, yet obviously we still have some problems.

I know also, Mr. Malfi, that your office conducted an investigation I think 2 years ago was it. If you could, briefly describe that investigation.

Mr. MALFI. We were requested to test the security at various government buildings and airports. We undertook an operation, undercover operation where we used false police credentials in an effort to obtain access into these buildings and bypassing the magnetometers and x-ray machines, carrying in briefcases to simulate the fact that we could have brought in weapons, explosives into these buildings.

We attempted 19 entries in the Washington area, and were successful in all 19 entries. We attempted two airports, and obtained entry into both airports, circumventing the magnetometers and x-ray machines in all the instances where we went out.

Mr. BARR. Were steps taken subsequent to that investigation to correct the deficiencies that investigation uncovered?

Mr. MALFI. After we completed the investigation we had again a debriefing with the agencies that were involved, and they instituted immediate steps to try and correct the measures that made it allowable for us to circumvent their security. So there was much concern about it, and the agencies reacted to this and put in certain policy changes to effectively enhance their security measures.

Mr. BARR. I want to make sure that Mr. LaTourette and the public and we understand exactly the scope of what you were able to do here, but also to indicate as I would like you to whether or not there were in fact areas of these Federal buildings—and we see pictures of the Federal buildings with many, many agencies housed

therein, and many thousands of Federal employees—it is my understanding that you were able to gain access to each one of the I think actually four buildings that you sought to penetrate; is that correct?

Mr. MALFI. That is correct.

Mr. BARR. And the identification cards that you were able to secure based on pretexts, that is false stories which apparently were not checked out; is that correct?

Mr. MALFI. That is correct. No due diligence was done in regards to the story that we used for the reasons we needed a building pass. We were able to obtain—Agent Cooney was able to obtain two legitimate building passes. From those legitimate building passes we counterfeited building passes for our other agents to gain infiltration into these buildings as a group, and then we went and on the strength of some counterfeit passes, building passes, we were able to obtain a legitimate building pass. So in turn through a ruse we got genuine building passes, counterfeited them, were able to get entry into the buildings using the counterfeited building passes, get access to the buildings when they were closed and after hours, and based on the strength of a counterfeit building pass we were able to obtain genuine building pass. So we would have eventually turned all of the counterfeit credentials, counterfeit building passes we had into legitimate passes.

Mr. BARR. Of course if one of our law enforcement agencies were conducting a true undercover operation, or an intelligence operation, you are familiar with the concept of backstopping; correct? In other words, if you are going to send an agent out in an undercover capacity you will backstop so that steps are taken down the line so that if his story is checked out it appears to be legitimate.

Mr. MALFI. Absolutely.

Mr. BARR. Their undercover operations are backstopped. You did not do that in this case; is that correct?

Mr. MALFI. Actually there was no need for us to do that in this investigation because nobody checked, pulled back the first layer. We had a system set up that in case we needed some verification for the fictitious stories that we laid out that we would have been able to provide that. But it was not necessary in this case.

Mr. BARR. In other words, there was not one call or effort made to check out the veracity of what you told the individuals in order to secure the passes or the codes?

Mr. MALFI. That is correct.

Mr. BARR. Thank you. Mr. LaTourette.

Mr. LATOURETTE. Thank you very much. Mr. Chairman.

Mr. Malfi, did you or your team actually carry explosives or firearms into these buildings?

Mr. MALFI. No, we did not.

Mr. LATOURETTE. And Mr. Barr asked one of the questions, but all of you have extensive law enforcement experience, each over 20 years if I heard you correctly earlier. Some missions that you are assigned to I assume are very, very difficult, some are very, very easy, and like the three bears some are in the middle I guess. How would you characterize the difficulty that you had in accomplishing what you did here in Atlanta?

Mr. MALFI. I would say we did not have much difficulty accomplishing this assignment. Even though there were some technical things that we had to do, we had to counterfeit the passes, but we used basic computerized software to do this, and it was not really that difficult.

Mr. LATOURETTE. And again basic computer software, is there anything extraordinary, any lengths that you had to go to, to recreate the passes that you have shown us here today? Anything—could Mr. Barr and I do this if we knew how to work a computer?

Mr. MALFI. I believe so. I mean the original pass was scanned, which is a common technology now that is used for computer printing. It was scanned in, it was worked on a little bit to get the colors as close as possible, and basically it was printed out.

The holograms which is a security feature, which is a good security feature, that appeared on the genuine passes. We did not duplicate—I mean we could have went through a more high scale type of technology and could have gotten holograms produced. I mean you can replicate that type of technology, but we did not go that far. We strictly produced a flat hologram that had the appearance if you just looked at it one way that it looked like there was something there, but it did not do the effect that an actual hologram does, which is when it hits the light reflects different colors to it.

Mr. LATOURETTE. In our earlier discussions with Ms. Sims and Mr. Shingler it came up that each building has a committee I guess set up to determine what security is maintained, it is a security committee; is that correct?

Mr. SHINGLER. Yes, sir. One of the recommendations from the original Department of Justice vulnerability assessment that Congressman Barr referenced was the establishment of building security committees. Those committees are made up of the tenants of the building, and they are each represented, each member is represented.

Mr. LATOURETTE. Is the adoption of security committees for each building something again that came out of this DOJ report?

Mr. SHINGLER. Yes, sir.

Mr. LATOURETTE. Is it required?

Mr. SHINGLER. It is required, yes, sir.

Mr. LATOURETTE. Let me ask you this. Could the General Services Administration mandate through rule or regulation what level of security is in each building?

Mr. SHINGLER. Could we, sir?

Mr. LATOURETTE. Yes.

Mr. SHINGLER. Yes, sir.

Mr. LATOURETTE. Are you aware of any—Ms. Sims, let me ask you this for the buildings that you are in charge of—are you aware of any security committee that has adopted a recommendation that everyone that enters the building go through the magnetometer?

Ms. SIMS. I am not aware of that recommendation.

Mr. LATOURETTE. Let me ask you, Mr. Malfi, I indicated before where Mr. Barr and I work everybody goes through the machines, and the reason is that we have former staffers that are no longer working on the Hill that do not turn in their credentials and can gain access to the building, and for security purposes we ask every-

body to go through the machines, and people understand that I think.

Is there any reason that—well, let me ask you this: If that had been the policy at these buildings you obviously could not have carried in briefcases and valises and other things without going through the magnetometers.

Mr. MALFI. That is correct. The whole purpose of us getting the building pass was after we did the surveillance on the buildings we realized that people that had the building passes were not subject to go through the magnetometers or to have their belongings x-rayed. So our purpose was to obtain a means in which we could bypass the magnetometers and x-ray so we could if we wanted to bring in weapons and explosives into the building.

Mr. LATOURETTE. And you talked about the fact that you had been here before, before you engaged in the attempt to get passes, and I guess I would ask you the same question. Did you spend an unusually long amount of time for a law enforcement operation casing the joint before you reached the conclusions you did necessary to breach the security of these buildings?

Mr. MALFI. No. We did this fairly quickly. I think it was two visits that it took us here. Manpower-wise it took about 3 days before we were ready to come back and actually do the operation.

Mr. LATOURETTE. Mr. Shingler, Steve Perry who is the Administrator of GSA has made some observations relative to the Federal Protective Service which is under your care and direction. One of the things that he has noted at least to me in another capacity that I have is that there is a pay differential that is hard the make up for the Federal Protective Service, and the one example that he cited was that there is a $10-an-hour difference between what someone can make working for the Capitol Hill police force as opposed to the starting wage in your salary. Is that an accurate observation?

Mr. SHINGLER. Yes, sir, very accurate.

Mr. LATOURETTE. Does that create a turnover problem for you?

Mr. SHINGLER. Yes, sir, constantly.

Mr. LATOURETTE. And likewise it is my understanding that you started, if not this year, a little while ago with 600 FTEs, full time FPS workers, and now you are down to the neighborhood of 450?

Mr. SHINGLER. Yes, sir. Turnover is tremendous.

Mr. LATOURETTE. Has the GSA put together, worked with the administration in a way to develop legislation to help correct some of the deficiencies relative to first pay scale, and second training?

Mr. SHINGLER. Yes, sir, we have.

Mr. LATOURETTE. And can we anticipate that in the near future?

Mr. SHINGLER. I would say yes, sir.

Mr. LATOURETTE. And the other deficiency that came up in some of the hearings, and this was principally brought to our attention by the officers within the Federal Protective Service is that there is a variation in the training that some of the contract guards are subject to in order to be under contract. Is that an accurate observation?

Mr. SHINGLER. Yes, sir. As a matter of fact, we have an active effort to bring some balance to that training effort, including a

drastic increase to that training in what we are going to call our building security guards, yes, sir.

Mr. LATOURETTE. And, Mr. Malfi, back to you. It is my understanding that the equipment was in place at all of these buildings, and people were in place in all of these buildings, and the breakdown I guess would be two, and I would like your comment, one is that when you have a policy that as long as you have one of these you can bring anything into the building that you want without having it checked, I would consider that to be a deficiency, and second of all the deficiency appears to be human error, that you were permitted to get through with credentials that were phony, and in one instance where you had even switched pictures with the other fellow.

Mr. MALFI. Exactly. Basically Congressman Barr brought this out earlier in his opening statements, that common sense and diligence is really the key to security, and as long as you have people that are watching but not paying attention, or looking and not seeing these type of vulnerabilities will continue to be a problem.

Mr. LATOURETTE. And last Mr. Shingler and Ms. Sims, it is not appropriate to talk about the recommendations that are attached in the confidential report that followed the briefing that you received, but I think that the fellow that issued is named Constable which is a good name I think for someone involved in law enforcement, but have you reviewed each of you all of the recommendations contained in that?

Mr. SHINGLER. Yes, sir, we have.

Ms. SIMS. Yes, sir.

Mr. LATOURETTE. OK. And I would just indicate, and again I do not think that we should try and surprise people, but I would just indicate that upon my entrance to this building, re-entrance that I found that the recommendations contained in Mr. Constable's report are not being followed, and I am sure that you will take that to heart and do what is necessary to fix it.

Mr. SHINGLER. By all means, sir.

Mr. LATOURETTE. Thank you very much. Thank you, Mr. Chairman.

Mr. BARR. Thank you, Mr. LaTourette.

It is my understanding that currently FPS, or the Federal Protective Service is under the control of the Public Building Service, and does not function as a truly independent security advocate for Federal facilities. Has the GSA ever considered moving the FPS out from under the Public Building Service to allow it to function truly as a law enforcement agency?

Mr. SHINGLER. We actually are very close to that as of this moment. The GSA did realign all of the regional offices, much as this one is, reporting to headquarters. In days past they used to report to the region itself. Now the Federal Protective Service is controlled out of the central office headquarters in Washington. Although we are part of the Public Building Service, we are a fairly integral part of that effort because a lot of what we do requires funding, and it is funded out of the Federal building fund. The Federal building fund is controlled by the Public Building Service. So we are a totally dedicated service as of this moment, and we do rely on the

funding mechanisms of the Federal building fund which are controlled by the Public Building Service.

Mr. BARR. The funding is very important, and as both Mr. LaTourette and I mentioned earlier, the Congress certainly has the responsibility there to make sure that all of these functions are funded properly.

I am not so much interested in the funding mechanism as separating FPS out so that it truly can function as a law enforcement agency.

Mr. SHINGLER. We have complete authority as of this moment, sir, to do that. I have never had—in the 2-months that I have been here already we have not had any interference whatsoever to try to do exactly as you said, to be a full-fledged at-the-table law enforcement agency.

Mr. BARR. Mr. Malfi, in your experience both in law enforcement and in these type of investigations involving Federal facilities do you see that it would help at all—and this is something we are looking at from a legislative standpoint as well I suppose—to separate FPS out and give it more autonomy as a law enforcement agency, as a separate entity?

Mr. MALFI. Actually I have not thought about or looked into that aspect of it, and I know GAO has not looked at that, but based on my experience if you have people that are involved in law enforcement that are involved in security and they are answering to people of the same culture with a law enforcement background things normally seem to run better for that arena based on the culture and the experience level that you have.

Mr. BARR. With regard to the meeting that you had immediately following the conclusion of the undercover phase of your investigation, have steps been taken, Mr. Shingler and Ms. Sims, since that time, just I guess a little over a month ago—actually when was that meeting, Mr. Malfi?

Ms. SIMS. March 20th.

Mr. MALFI. March 20th.

Mr. BARR. So just about a month ago. And, by the way, let me say we appreciate your doing that, even more important than getting your information, or even physically getting back up to Washington you sat down with the agencies here because you perceived that there was a very serious problem, something of which they should be made aware of immediately, and I think that is very appropriate and commendable.

In followup to that, Mr. Shingler and Ms. Sims, could you again without revealing any sensitive law enforcement techniques, tell us some of the steps that have already been taken to address the deficiencies that GAO discovered.

Ms. SIMS. Let me just say that during that March 20th meeting one of the first things that Agent Malfi said to us is that there has never been a facility that he has set his sights on that he has been unable to penetrate, and that is evidenced by his testimony in which he said that he has been able to penetrate 19 Federal facilities and two airports.

We at the U.S. General Services Administration take no consolation in being lumped into that group. We do not make an excuse by being lumped into that group now.

But what I will say is that within hours of that March 20th meeting we took immediate, decisive, and what we believed to be effective steps, probably a dozen steps to further improve security postures in the Federal facilities, and we are currently working on at least a dozen more. And that is in addition to what we have always done prior to September 11th, prior to the penetrations by the U.S. General Accounting Office.

Some of those that we have been doing would include security surveys, would include occupant emergency planning, would include building security committee meetings, would include daily contact with the tenants and visitors, and implementing the feedback that they give us each and every day.

Mr. BARR. Two of the items that Mr. Malfi discussed and that his colleagues have mentioned also, though, would seem to be of the sort that would not require a serious problem like this in order to be directive.

Both prior to and after this investigation will all of those folks under GSA's or FPS's authority actually look at a badge physically to determine that it is in fact, or that at least it appears to be in fact a valid identification pass?

Ms. SIMS. Yes, sir. We employ a three-step process by which we look at the badge, we look at the face of the individual, and we look again at the badge, and we are confident that those strategies are currently being employed.

Mr. BARR. That was not the case, though, obviously prior to the undercover investigation, that three-step process obviously was not used.

Ms. SIMS. I believe that it was used in most cases. Security is a very unforgiving discipline, and it requires daily iterative follow-up, and that includes meeting one-on-one with contract security guards and the contractor to reiterate what the ongoing policies and procedures are.

Mr. BARR. With the particular badges that you have described, if somebody, Mr. Malfi, had simply looked at it even cursorily and seen that it did not have the proper hologram on it for example, how many times were collectively you all able to secure access to Federal buildings based on those badges?

Mr. MALFI. I believe if they would have looked at the badges first of all they would have definitely caught the fact that I was using John's building pass because his photograph appeared on it, not mine.

If they also looked at the passes, all of the counterfeit building passes should have been detected and those people should not have been not allowed entry, and a followup investigation should have occurred. So in all instances——

Mr. BARR. But about how many times did that occur?

Mr. MALFI. On almost all of the entries that we made.

Mr. BARR. I mean a number of times?

Mr. MALFI. We infiltrated the buildings I think on two occasions. We went back twice. I mean because once we got through then we wanted to go through at night time with the crew, you know, with the group, and we saw no need to continually, you know, for 3 weeks straight go in and out of these buildings. Once we pene-

trated it, we got inside, you know, that operation was over as far as we were concerned.

So I believe there was like two penetrations for most of the buildings, and one penetration for another.

Mr. BARR. By each one of you?

Mr. MALFI. That is correct.

Mr. BARR. So that would mean at least six penetrations?

Mr. MALFI. Six, and then we had two other undercover agents that also went into the buildings.

Mr. BARR. And in not one of those instances was the badge physically inspected?

Mr. MALFI. That is correct.

Mr. BARR. This is the problem that we have, Mr. Shingler. It may be your belief or your wish that in most instances that simple step occurs, but apparently in none of these instances—I mean it is not as if they were stopped most of the time and looked; it was never looked at. Is that a concern?

Mr. SHINGLER. It is deeply a concern. Policies are one thing, all the equipment in the world are another just as Mr. Malfi said. And I was at the hearing the other day that his counterpart was at. All the technology in the world is not going to do you any good if your staff is not there and trained to identify it and do something with it. We feel that is a key for us, and training and getting the proper staff is definitely going to be one of our major efforts. I have already spoken to Mr. Malfi about—the Federal Protective Service faces a lot of challenges. This effort has helped us focus and set priorities for addressing those challenges, and that is what we are attempting to do, sir.

Mr. BARR. When an initial approach is made as Mr. Malfi and his colleagues did in order to secure an initial pass, building pass, and a story is told that obviously is not true, is there a process now in place that obviously was not in place before so that in every instance that story is checked out at least one level?

Mr. SHINGLER. Yes, sir, that practice is in place now. I think for the most part most policies were in place, although we have issued further policy guidance. It was the actual doing the work, and it is great to talk the talk, but walking the walk is the thing, and we just were not totally walking the walk at that point, and I think we are now, sir.

Mr. BARR. As a result of the briefing on March 20th and this operation generally, have you all been able to identify particular individuals that committed serious breaches of security and allowed this to happen, allowed these penetrations to occur and these false badges to be used?

Mr. SHINGLER. I misunderstood the question, sir.

Mr. BARR. Have you been able to identify particular individuals who fell short of the standard that you all maintain?

Mr. SHINGLER. Employee-wise, or contractor-wise?

Mr. BARR. Yes.

Ms. SIMS. Yes, sir, we have.

Mr. BARR. And has action been taken to correct those situations?

Ms. SIMS. Yes, sir, it has been.

Mr. BARR. Have persons been terminated?

Ms. SIMS. No, sir.

Mr. BARR. Have any contract personnel been removed from those responsibilities?

Ms. SIMS. Yes, sir.

Mr. LATOURETTE. Mr. Barr was talking about the new technology, and let me just ask if you are based upon your experience aware of any additional security technologies including smart cards or biometric devices that you think could be used to help eliminate some of the human error that was discovered in this operation, Ms. Sims, and then you, Mr. Shingler? Are any of those currently under discussion or consideration by the GSA relative to building security?

Ms. SIMS. Yes, sir. GSA in several regions across the country is currently employing pilot projects which utilize smart card technology. Certainly if we had our druthers the Nation would move toward that.

Mr. LATOURETTE. And just for the benefit of those that do not know what a smart card is, maybe you could just explain what it is that those pilot projects are doing.

Ms. SIMS. Well, there are variations on it. Up in New York several buildings utilize smart card technology in which the individual's—I am sorry. Wendell, would you like to——

Mr. SHINGLER. Absolutely.

Basically what it is is it is an identification card with a computer chip inside, and within that computer chip could be a variety of pieces of information, the person's name, Social Security number, and a physical picture so that when it comes up on a computer screen and it is accessed through a reader you could doubly verify that it is the person on that card and in person in front of you. So there is a wide variety of checks within those pieces of equipment.

Biometrics is another issue that we are looking at. Again as I said in my opening statement I do not know that there is a silver bullet, but it is definitely one of those items that we intend to work with the Interagency Security Committee which is also from the vulnerability assessment that is a government sharing of information, and that is where we will address a lot of those areas, especially with the Defense Department who has done a lot of research into those areas.

Mr. LATOURETTE. I do not want to get too far afield from the subject of this hearing in terms of an internal penetration, but both what happened in Oklahoma City and at the World Trade Center had to do with things happening externally to buildings. Has GSA engaged in a study of the properties under its control relative to external security? Say the building we are sitting in today?

Mr. SHINGLER. Yes, sir. We are actively doing that in two methods. One, the new buildings that the Hill authorizes for new courthouses and the like, we are looking at new technologies and old technologies. We are putting seismic things, designing them into the building that probably were not used in years past in other than the seismic regions such as the West Coast. So we are looking at those things.

We have done a lot of research in glass. As you may be aware, in Oklahoma a lot of people were hurt or injured or killed because of flying glass, so we have done a lot in the scientific look-sees at glass.

We are also using a lot to address the existing buildings. We are looking at set-backs, how we can increase set-backs using street closures or lane changes, or even just changes to the surfaces of the buildings. So we are actively looking at all of those areas.

Mr. LATOURETTE. And actually one of the not-often-enough-told stories is one of the women who lost a child in the day care center in the Murrah Building and started a foundation called People First, and it has specifically dedicated itself to the development and research of shatterproof glass for not only Federal buildings but for also other facilities, and she is doing wonderful work.

And last, Mr. Malfi, maybe to impress, and I want to indicate that I guess what concerns me about the answer to Mr. Barr's question, again when I went outside the building not only did I get a second visitor's pass, but someone with a yellow pass just blew right past the guards and the magnetometer, no one touched the pass, nobody examined the pass, nobody matched up the picture, and so I know that you are in here and you have contracted with people to engage in security, but it appears to me that we are still not quite there, even in the fact that I assume most of the people in the building know what we are doing here if they watch television, so I would think that they would take it a little more seriously.

And maybe to give the matter some seriousness, Mr. Malfi, what was the biggest container that you or your agents brought in in terms of a suitcase that you could put in an overhead bin, or a briefcase?

Mr. MALFI. We took in a travel bag, a valise-type bag that could have been used to bring in certain equipment, certain explosives, anything basically we wanted to bring into the building.

Mr. LATOURETTE. And did any of you during the 20-plus years that each of you had with the Secret Service, do you have experience with explosives training?

Mr. MALFI. Enough to know to get away from them. That is about it.

Mr. LATOURETTE. Are you able to estimate or guesstimate based upon the size of the valise that you brought in what sort of damage you could have done to this building if it had been packed for instance with C4 explosives?

Mr. MALFI. Well, basically depending on where we would have placed those, how much we would have brought in. It depends. I mean once you have access to a building and free reign on the building then you can sort of accomplish basically anything you want to.

I do not think anybody would have stopped us if we all walked in carrying two large duffel bags each. I mean we had the building passes that allowed us to bypass the magnetometers and the x-rays. The main thing is that technology is not a cure-all for security, money is not a cure-all for security. The bottom line is that due diligence is really the most vital factor in regards to any type of security that you have set up.

People have to be diligent in what they are hired to do, they have to adhere to the policies and understand why those policies are in effect so that it makes sense to them so that they could prevent things like this from going on.

Mr. LATOURETTE. And part of that is not only going over things, but it is training, and it is also compensating somebody at a rate that motivates them to do their job I would assume.

Mr. MALFI. That is correct.

Mr. LATOURETTE. Thank you very much.

Mr. BARR. Going back, Mr. Malfi, to the one aspect of the badges, you say there was the designation on the badges that allowed the person, or indicated that the person possessing the badge could carry firearms into the building. What was done in order to secure that additional authority?

Mr. MALFI. Basically Agent Cooney just did a little social engineering in regards to having that person put that extra feature on that badge.

Mr. BARR. In other words, he just gave them a story that he needed to carry a firearm?

Mr. MALFI. In the conversation it came up that he may need this, and he says, yeah, he says I definitely could use this, and they put it on. So it was volunteered, right, John?

Mr. COONEY. Correct. I did not have to explain in detail what the need for a firearm was. I just said I would be coming in with firearms at some time, and they said "Well, then you need this feature on it," and I said "Yes, I would like to have that." They were very willing.

Mr. BARR. What steps have been taken to correct that particular deficiency in the wake of this investigation? Ms. Sims.

Ms. SIMS. Would you elaborate on the question, please?

Mr. BARR. Not really on the question, but what steps have been taken to address that particular deficiency? In other words, the ease with which the undercover officer was able to get the designation on the badge that allowed them to bring firearms in without having to explain or provide any sort of documentation at all.

Ms. SIMS. Without getting too detailed on our security protocols, there are at least a half dozen steps that we have taken specifically to that element of building entry. One would include tightening up the policies and procedures associated with the issuance of the badge. The actual badge issuance procedure has changed in terms of who issues the badge, the actual application for the badge has changed, and the validation process by which we issue the badge has changed and tightened up.

Mr. BARR. We have been talking generally today very specifically about the facilities here in Atlanta in Region 4. Are the measures that we have been talking about here today being implemented across the country in all regions of the country, in all facilities under the jurisdiction and control and responsibility of GSA and FPS?

Mr. SHINGLER. The specific ones that are being done here may not necessarily be, but the intent is each of Sabina's counterparts, the regional directors in the balance of the country are specifically addressing similar types of issues.

Some of the ID card issuance procedures are different from location to location, but the ultimate intent of tightening up our security of getting in and out of buildings is definitely being addressed nationally, sir.

Mr. BARR. I mean it would seem to me that what we are talking about here is just so basic, namely not just giving somebody a designation to carry a firearm into a Federal building without asking any questions or checking anything out, but the issue of simply checking to see whether the person that they say they are coming to see actually needs to see them, physically looking at a badge, and these are all so basic I am somewhat at a loss to understand why we cannot have the assurance today that they are in fact being implemented in all GSA regions for all Federal buildings.

Mr. SHINGLER. No. Absolutely, sir. I misunderstood what you were asking. Yes, sir, that is happening. They have tightened up security nationally. I misunderstood what you were talking about, the holograms and one thing or another.

Mr. BARR. So as we sit here today can you assure us in the Congress and the American people that at least these specific steps that we have identified here today as being deficiencies in Federal building security are being addressed, have been addressed, and will continue to be addressed properly?

Mr. SHINGLER. Yes, sir.

Mr. BARR. Ms. Sims.

Ms. SIMS. Absolutely.

Mr. BARR. We talked earlier about the different levels of security for the Federal buildings, and we have pictures of the different Federal buildings, at least five of them here in the Atlanta area. What is the level of security for each one of these buildings?

Mr. SHINGLER. They are all Level 4 facilities.

Mr. BARR. And if you could just explain briefly what Level 4 means.

Mr. SHINGLER. The vulnerability assessment, the DOJ vulnerability assessment categorized virtually all Federal buildings in one of five levels. Primarily the first four, 1 through 4, are the ones that we deal with. The fifth level are those agencies such as the Pentagon, or the CIA headquarters where they may employ their own security requirements. But the 1 through 4 levels are based on a variety of things, primarily how many people are in them, the size of the building, the type of mission that goes on within the building, the threat assessments that could happen, from the shopping center type of recruiting office all the way to a building of this magnitude here in Atlanta. So that is where they range between the 1 through 4 levels.

Mr. BARR. The buildings earlier, in your earlier investigation 2 years ago, Mr. Malfi, were they all Level 4 facilities?

Mr. MALFI. I believe a lot of those buildings were Level 5.

Mr. BARR. In other words, even a higher level of security and vulnerability associated with them?

Mr. MALFI. That is correct.

Mr. LATOURETTE. Mr. Shingler, if I could just have one more sort of housekeeping question, Mr. Barr was talking about where the money comes for the Federal Protective Service, and it does come from the Public Building side of GSA, and it is my understanding that the tenants, for instance if the Internal Revenue Service is in a GSA-operated building that they pay you so much per square foot or whatever to provide security. Am I right about that?

Mr. SHINGLER. Yes, sir. For the most part there is an across-the-board charge, and each square foot of rent an X percent goes to security. And then there are building-specific charges that are added onto that which in some cases there are multiple entrances that they may want to have guards at, or anything that is above what the basic security charge covers.

Mr. LATOURETTE. And GSA could by regulation—we have already I think said this—but GSA by regulation could require everybody that comes into this building to go through the magnetometer, but you have chosen not to do that, you have chosen to leave it up to the security committees.

Mr. SHINGLER. Yes, sir.

Mr. LATOURETTE. I think I would ask you to chat with Mr. Perry and see if that could be reevaluated. But likewise are there lease arrangements because not every building that you operate is a government-owned building, there are also leased buildings that you lease on behalf of the government. Are there restrictions by landlords, or are there lease restrictions that somehow impede your ability to protect the men and women of the Federal work force and the people that visit them?

Mr. SHINGLER. Balancing security with openness is a primary issue that we are constantly addressing. One of our biggest challenges right now are leased facilities, but we are working closely with the Interagency Security Committee to come up with a minimal standard to implement security in leased locations.

We are also working with organizations such as BOMA, Building Owners and Managers Association, to come up with standards that not only they can live with, but meet our needs of protecting our government employees. So we are actively addressing those issues, sir.

Mr. LATOURETTE. Are any of the buildings that we are talking about today in Atlanta leased, or does the Federal Government own them all?

Ms. SIMS. We own them all.

Mr. LATOURETTE. You own them all.

Ms. SIMS. Yes, sir.

Mr. LATOURETTE. Thank you very much.

Ms. SIMS. Excuse me, let me correct. The Sam Nunn Atlanta Federal Center is a complex lease-to-own financial deal. At the end of a period of time we will own that facility.

Mr. LATOURETTE. But do you currently on behalf of the Federal agencies that are located there, do you lease it from someone at the moment?

Ms. SIMS. Yes, sir.

Mr. LATOURETTE. OK. Are there any restrictions—I guess that is what I want to get to—are there any restrictions in the lease that prevent you or hinder you from engaging in the security that you engage in in a wholly owned Federal building?

Ms. SIMS. At that facility no. That facility is operated as if it were ours from a security stance.

Mr. LATOURETTE. Thank you very much.

Ms. SIMS. Sure.

Mr. BARR. The investigation, the undercover investigation that took place in early March, and we have identified what I presume

we would all agree are serious security problems, the failure to look at a badge, the ease with which somebody gets the badge based on a false pretense that was not checked out, the additional volunteering of the designation to be able to carry firearms in, agents giving an access code to these undercover agents without checking them out properly, would everybody here agree that those things should not have occurred?

Ms. SIMS. Yes, sir.

Mr. BARR. What specific steps—and were those problems, were those errors made by both contract personnel and FPS employees?

Ms. SIMS. Employee singular, and contract employee singular. Yes, sir.

Mr. BARR. And are there any limitations under which GSA or FPS now operates that would prevent effective disciplinary action being taken against either employees or contract personnel for identified security lapses such as these?

Ms. SIMS. The contract employee referenced in the scenarios no longer provides the service to the U.S. General Services Administration.

With respect to the GSA employee, that employee has been reprimanded.

Mr. BARR. Is that sufficient in your view? Are there—I guess I am asking a more general question. Are there any limitations under which you all have to operate now that would prevent you in any way from taking what you believe is effective disciplinary action against an employee that commits a serious error in security? Do you have sufficient authority?

Ms. SIMS. Yes, sir, we do.

Mr. BARR. Does that include termination of an employee?

Ms. SIMS. If it were deemed appropriate, yes, sir, it most definitely would include up to termination.

Mr. BARR. OK. And you do have the ability to terminate the services of a contractor similarly, and you have plenty of authority to do that?

Ms. SIMS. Unilaterally and very quickly.

Mr. BARR. Thank you.

Do any of you all have anything additional that you would like to add for the record today that we might not have gone over, or to supplement anything that we have touched on today?

Mr. SHINGLER. We appreciate the opportunity to be here.

Mr. BARR. Thank you.

As I indicated—do you have anything else, Mr. LaTourette?

Mr. LATOURETTE. I do not. Thank you.

Mr. BARR. Counsel?

As I indicated, the record will be kept open for 10 days so that if there are any additional materials that you would like to submit.

And let me ask just one final question I forgot. With regard to followup measures, is this an ongoing process, Mr. Shingler or Ms. Sims?

Mr. SHINGLER. We will constantly be following up, because weapons and terrorist activities have changed drastically. Hopefully we will never be able to sit here and say we have done everything we could do, because we will constantly adjust to that.

Mr. BARR. Now, we have purposely not gone into in this public setting all of the details of the security breaches, which is good both from the standpoint that we have not indicated a specific road map or game plan that somebody could use, and I think people would be shocked even at some of the details that we did not go into here, the ease with which the security breaches were effectuated, but knowing, Mr. Shingler and Ms. Sims, as you do the full details of this undercover investigation here, can you assure us that if that same operation were carried out tomorrow it would very clearly not succeed?

Mr. SHINGLER. Yes, sir, I can say that.

Mr. BARR. Ms. Sims.

Ms. SIMS. I am confident that we have taken the steps that we need to take, and that we are continuing to take the daily iterative steps that we need to protect the people and the properties, and the daily visitors who frequent our facilities.

Mr. BARR. I mean this is not a trick question at all. I am just wondering if as you sit here today you feel confident that if this same type of operation were carried out tomorrow that it would not succeed. Do you feel confident in that?

Ms. SIMS. As I said, I am confident in the fact that we have done everything, and we continue to do everything to protect the people and the properties.

What is a little bit frustrating is that with the state of technology today is it difficult to discern fake identification.

Mr. BARR. No, it is not. I mean that is the whole point of this hearing. I mean it is not. This is one that has the proper hologram, this is one that is not. It is not difficult to tell that one does not have the proper hologram and that one does.

Yes, there certainly other aspects of falsification of identification that are much more difficult to discern, you are absolutely correct, but the undercover operation that was effected here is something that a high school student—I mean no insult to these gentlemen, but they especially and consciously dumbed down their operation. Is that correct, Mr. Malfi, that you sort of dumbed it down, you used the lowest level of technology to thwart the security measures; right?

Mr. MALFI. Correct. To duplicate the building passes, like I said, we did not use anything that was sophisticated. We used something that was accessible to the general public.

I mean we could have—with the technology that is available to us we could have duplicated these things very, very close to the originals. That was not our intent. Our intent was to give basically a fighting chance to show that if somebody paid attention to these things it would have been detected.

Mr. BARR. And that is sort of my point, Ms. Sims, and I come back to it again. I am not talking about the more sophisticated measures that somebody might come up with and that we have to be continually on guard against, just with regard to these most elementary measures that thwarted security measures at Federal buildings here in Atlanta, can you give us your assurance that at least this level of threat has been taken care of and if this type of operation, not a more sophisticated one, and we hope the answer would be the same for that, but just for this level of security breach

are there measures in place today so that if the same type of operation were attempted tomorrow you feel confident that it would not succeed?

Ms. SIMS. Yes, sir, I am confident that the scenarios employed would not meet with the success before, yes, sir.

Mr. BARR. OK. We appreciate very much the time and effort that our witnesses from GAO put in in traveling down here, and we also appreciate very much the swift response and continuing effort by Mr. Shingler, Ms. Sims, and their colleagues and the other Federal agencies in addressing these problems.

And with that I would like to thank Mr. LaTourette for traveling here from the great State of Ohio today and being with us. I appreciate counsel and the committee staff for all of the preparatory work here, and I hereby declare this hearing of the Government Reform Committee closed.

[Whereupon at 11:55 a.m., the committee was concluded.]

[Additional information submitted for the hearing record follows:]

GSA

GSA Office of Congressional and Intergovernmental Affairs

June 28, 2002

The Honorable Bob Barr
U.S. House of Representatives
1207 Longworth House Office Building
Washington, DC 20515

ATTENTION: Joshua Gillespie

Dear Representative Barr:

Please find enclosed the responses to the follow-up questions submitted to Wendell Shingler, Assistant Commissioner, Federal Protective Service, Public Buildings Service, General Services Administration from the hearing held on April 30, 2002 in Atlanta on security at Federal buildings.

Should you have any further questions regarding this matter, please have a member of your staff contact Wendell Shingler on (202) 501-0907.

Sincerely,

Shawn McBurney/SP
Shawn McBurney
Associate Administrator

Enclosures

U.S. General Services Administration
1800 F Street, NW
Washington, DC 20405-0002
www.gsa.gov

The Office of Federal Protective Service (FPS) responses to your questions follow:

Question 1: (a) Explain in detail the process Federal employees must go through to obtain a building security pass before and after the GAO investigation. (b) Does this process apply to all Federal facilities across the nation? (c) What is unique to this process for Federal employees in Atlanta?

Response:

1(a) – The issuance process for building passes/access control cards prior to, and after (*) the GAO investigation is as follows:

1) The agency representative requesting the identification (ID) card completes the Southeast Sunbelt (SESB) Region ID card request form. The form is then signed by a designated official (Requesting Official) from the requesting agency.
2) Once the form is completed and signed, the employee or agency representative requesting the ID card submits the form for processing.
*3) The requesting employee isrequired to present another form of official ID when he/she reports for the issuance of the ID card.
*4) The FPS official issuing the ID card verifies the information on the request form by the requesting agency. Thereafter, they complete the FPS portion of the form prior to issuance of the ID card.
*5) The FPS official will issue the identification/access card upon verification of the request and positive identification of the requesting employee.

Note:*Steps 3-5 above were added after the General Accounting Office (GAO) investigation.*

1(b) – No, the process used in Atlanta does not apply to all Federal facilities nationwide. The actual process for issuing building passes/access control cards will vary in each facility. However, each process will comply with the minimum security standards recommended in the June 28, 1995 Department of Justice (DOJ) "Vulnerability Assessment Report of Federal Facilities."

1(c) – The unique aspect of this process for Federal employees in Atlanta is that the FPS regional office in Atlanta, Georgia, now has mandatory accountability controls for the protection of ID cards and credentials, un-issued cards, and non-photo passes.

Question 2: Upon completion of the undercover investigation, GAO investigators provided representatives from GSA, the U.S. Attorney's Office, and the Marshals Service, a detailed briefing on the results of the security tests and identified the weaknesses found. A copy of the GSA meeting notes taken from that briefing has a section entitled "Region 4's Immediate Steps," which states that all ID badges will become an FPS function, executed by an FPS employee. Prior to this, whose function was it, and did FPS have any oversight or managerial role of the issuance of badges?

Response: The function of ID badge issuance was formerly the responsibility of the GSA
Public Buildings Service (PBS), Office of Property Management, through contract employees. FPS had no oversight or managerial role.

Question 3: In the same, above-mentioned section from the meetings notes memo - "Region 4's Immediate Steps", it states: "FPS will reproduce badge applications from the last three weeks and print out from the badge system information on all issuances. From there, FPS will research issuances and cancel fraudulent PIN issuances and share names with FPS counters and GSA leadership." Please provide a listing of all the "fake names" shared with FPS counterparts gleaned from the badge applications.

Response: As stated in the meeting notes, FPS did conduct such a three-week review. Based on this review no fraudulent badge applications were identified and, as a result, no "fake names" were identified or shared. The photo of Agent Sullivan and the Personal ID Number (PIN) issued him were deleted from the ID Manager system.

Question 4: The meeting notes also states that "FPS will review film footage for possible photos of Agents Malfi and Sullivan for dissemination on a need to know basis." (a) For what reason did FPS decide to dedicate its time to pursuing Agents Malfi and Sullivan, as opposed to addressing the security weaknesses? (b) Was film footage of any of the GAO agents circulated? (c) If so, specifically to whom and for what purpose?

Response:

4(a) – Contrary to what was transcribed as meeting notes, neither PBS nor FPS reviewed the film footage in question. However, FPS did develop an action plan immediately after the incident and began implementing measures to mitigate related security weaknesses.

4(b) and 4 (c) - No film footage was retrieved or circulated.

Question 5:(a) Please provide the name of the individual who drafted the above-mentioned memo; (b) a list of names and offices to which this memo was sent; and (c) the means by which this memo was delivered (i.e., fax, email, airmail). Given the sensitive nature of the memo, and the detrimental consequences that may have resulted should it have landed in the wrong hands, GSA has initiated an investigation into this matter. (d) Please provide and update on the status of this investigation.

Response:

5(a)(b)(c) –This question refers to an alleged memo that was purportedly drafted by a GSA official. Although we are unaware of such a memo, the day following the GAO briefing to GSA, several GSA's officials from Region 4 and Central Office did meet to discuss the facts of the GAO investigation and to determine potential corrective actions. As requested by the SESB Regional Administrator, the SESB FPS Regional Director transcribed discussion from this meeting to informal, written meeting notes. These written notes were then distributed, via fax, only to those meeting participants, who included SESB Regional Administrator, SESB FPS Regional Director, FPS Assistant Commissioner, PBS Deputy Commissioner, GSA Congressional Affairs, and GSA Public Affairs.

5(d) – The GSA IG investigation has been completed and is under review by the FPS Assistant Commissioner.

Question 6: (a) Please provide a specific and detailed listing of the exact steps and measures undertaken by FPS to upgrade security following the undercover investigation, in which GAO exposed serious security breaches at Federal buildings in the Atlanta region. (b) Were these measures implemented throughout the country or in the Atlanta metro region only?

Response:

6(a) - Following the security breaches, FPS Region 4 immediately took the following steps:

1) Cancelled fraudulent ID badge and PIN issued.
2) Briefed senior management from affected facilities.
3) Issued a letter to guard contractors reiterating building entry policies and procedures.
4) Met with contract guard project managers of affected facilities to reiterate that positive ID checks be performed.
5) Implemented positive ID checks by contract guards (three step process).
6) FPS took responsibility for the issuance of ID cards and access control PIN numbers in the Atlantaarea and issued step-by-step guidance for the ID badge issuers.
7) Submitted action plan to GSA Regional Administrator and FPS Assistant Commissioner.
8) Conducted listening sessions with law enforcement managers from affected facilities.
9) Distributed region-wide letter on building access procedures for armed law enforcement personnel in GSA-controlled facilities.
10) Regional Administrator and FPS Regional Director held several discussions with senior heads from the affected facilities.
11) Reviewed ID and access control procedures throughout Region.
12) Enhanced law enforcement building entry procedures through the purchase and issuance of hologram for building ID cards.
13) Purged ID Badge Manager System of outdated data.
14) Conducted special BSC meetings tenants of each affected facility.
15) Identified supplemental funding requirements for human capital and equipment.

6(b) – These measures were implemented at facilities in Atlanta referenced by GAO. The following steps were taken on a National level:

1. Teleconference conducted with all FPS Regional Directors and Central Office staff to discuss incident and lessons learned.
2. FPS Assistant Commissioner advised all regional directors of the Atlanta incident and instructed them to inform their own staff of the incident.
3. FPS Assistant Commissioner instructed the regional directors to ensure that their respective staffs check their contract guards and ensure they follow building access control procedures.

Question 7: GAO investigators easily breached security because basic screening procedures were ignored. a) What specific disciplinary steps have been taken against the responsible employee(s) in the wake of these mishaps? b) If no disciplinary action with regard to any particular employee or contractor was taken, please explain why. c) Precisely what disciplinary steps or other measures were taken against contract personnel and their companies? d) Please furnish copies of any and all documents, including but not limited to contracts, regulations, letters, memoranda manuals, etc., detailing discipline and accountability for GSA and other Federal employees, or contract personnel, regarding security standards and breaches thereof.

Response:

7(a) – The FPS District Manager (first line supervisor) issued a written reprimand to the FPS official responsible for authorizing the issuance of the ID card to Agent Sullivan. This reprimand has been placed in the FPS official's personnel file.

7(b) and 7(c) – The contract employee responsible for the issuing of the ID card to Agent Sullivan was terminated by his employer. The contract for issuing ID/access cards was terminated effective June 6, 2002, and FPS has since taken over the issuance of the ID cards.

7(d) - See attached Documents:

(1) GSA Penalty Guide, Table 1 and 2, dated January 31, 1989. (Enclosure 1)
(2) Guard Contract Manual, dated April 2001. (Enclosure 2)
(3) Contract Guard Specification, Section H. (Enclosure 3)

Question 8: (a) How often do FPS and contract security guards receive training? (b) Does the training for FPS security guards and contract security guards differ? (c) If so, how?

Response:

8(a) – All security guard firms employed by FPS in GSA controlled facilities is accomplished through contracting. These contract employees receive training upon initial employment and refresher training every two years thereafter. For those contract guard employees that will be "armed", they will receive an initial forty hours of firearms training and qualification at an approved range. This weapons training/qualification will be followed by annual weapon re-qualification. Please refer to table listed below for listing of required training for both Productive and Supervisory personnel. For the various forms of annual training see the attached Guard Contract, Section J, Exhibits 4, 5 and 6 (See Enclosure 4).

PRODUCTIVE:

TRAINING COURSE AND HOURS	GOVERNMENT PROVIDED	CONTRACTOR PROVIDED
Basic Training – 72 Hours		**XXX**
FPS "orientation" training – 8 Hours	**XXX**	
Magnetometer/X-Ray Training (Applies only to screening posts) – 8 hours	**XXX**	
Annual CPR/First Aid Training and Certification		**XXX**
Re-certification Training – 40 Hours (Every 2 years)		**XXX**
Firearms Training – 40 Hours (Armed Guards Only)		**XXX**
Annual Firearms Requalification (Armed Guards only)		**XXX**

SUPERVISORY:

TRAINING COURSE AND HOURS.	GOVERNMENT PROVIDED	CONTRACTOR PROVIDED
Basic Training – 72 Hours		XXX
FPS Specific training – 8 Hours	**XXX**	
Magnetometer/X-Ray Training – 8 hours	**XXX**	
Annual CPR/First Aid		**XXX**

Training and Certification		
Re-certification Training – 40 Hours (Every 2 years)		**XXX**
Supervisory Training – 9 Hours		**XXX**
Firearms Training – 40 Hours (Armed Guards Only)		**XXX**
Annual Firearms Requalification (Armed Guards only)		**XXX**

8(b) – As stated in 5(a) above, FPS contracts with security firms for contract guards through several contractual vehicles. Training requirements for FPS contract security guards are developed nationally.

8(c) – Not applicable.

Question 9: (a) Has the FPS or the PBS considered implementing a policy whereby no individuals are allowed to bypass x-ray machines or magnetometers? (b) If not, why not?

Response:

9(a) – Yes, FPS has considered implementing such a policy nation-wide.

9(b) – However, based on results of this consideration, FPS has established policy that focuses on developing security packages that are building specific and are designed to reduce or eliminate credible threats identified for each building. To support this policy the minimum-security standards recommended in the DOJ Vulnerability Assessment Report are used as minimum guidelines for each GSA controlled building. Normally these minimum-security standards do not require Federal employees to be screened, e.g. pass through a magnetometer and have their hand carried items x-rayed. However, there are means to increase a building's minimum-security standard which include: 1) a terrorist event such as the 9/11 attacks, 2) specific recommendations from the Building Security Committee, or 3) FPS receives specific intelligence that would warrant the increase of the minimum-security standards.

Question 10: Please describe the number of companies and the number of contract personnel with which GSA contracted prior to the undercover investigation, in the Atlanta region, to perform security or security-related functions. (b) Describe the duties performed by these companies and the contract personnel. (c) How many such contractors and contract personnel are now utilized for security or security-related functions, by GSA in the Atlanta region, now?

Response:

10(a) - Prior to the undercover investigation, there were three security guard companies (with 237 contract personnel), one technology/management consulting firm (with eight contract personnel), and a Property Management Center maintenance contractor (with one person assigned) for ID badge issuance.

10(b) - Employees of the three guard companies provide building entry screening, access control and canine explosion detection services. The technology firm employees design intrusion detection systems and handle electronic systems repair and maintenance services. The maintenance contract employee issues the ID badges and after hours access PIN numbers.

10(c) - The same companies noted in 10(a) above continue to provide these security services. There are two exceptions – the first pertains to the maintenance contract employee, who was terminated by their employer immediately after discovery of the incident and the second pertains to the maintenance contractor who was terminated by GSA for poor performance effective June 6, 2002.

Types of Delinquency or Misconduct	1st Offense	2nd Offense	3rd Offense
1. Reporting for duty or being on duty under the influence of intoxicants or drugs to such an extent as to render the employee unfit for duty. Also using or selling intoxicants (not controlled substances) on Government-owned or leased premises, or possessing intoxicants on Government property where such possession has been prohibited..			
a. Where safety of persons or property is not endangered thereby.	Warning notice to reprimand	Reprimand to removal	Removal
b. Where safety of persons or property is endangered thereby.	Suspension to removal	Removal	
2. Driving a Government vehicle (or privately owned one on official business) while under the influence of intoxicants or drugs.	Suspension to removal	Removal	
3. Use of illegal drugs by employees serving in positions designated for drug testing as confirmed by a positive test result or refusal to take drug test.	Reprimand to removal	Removal	
4. Recurring tardiness: Being late for work (up to 30 minutes) without adequate justification. A penalty action may be imposed whenever 3 unexcused tardinesses occur within a period of 2 months or less.	Warning notice	Reprimand to suspension	Suspension to Removal
5. Absence from duty for one day or less without permission and without adequate justification; failure to follow instructions for notifying supervisor or obtaining approval for absence. (includes tardiness of more than 30 minutes and leaving the job without permission.)	Warning notice	Reprimand to suspension	Suspension to Removal
6. Absence from duty for more than one day without permission and without adequate justification or failure to follow instructions for notifying supervisor and	Warning notice to reprimand	Reprimand to removal	Removal

Figure 3-112.1. Penalty Guide, Table I
(Part 1 of 3)

Types of Delinquency or Misconduct	1st Offense	2nd Offense	3rd Offense
obtaining approval for absence. (When absence exceeds 10 calendar days without permission and without adequate justification, the penalty of removal may be imposed for the first offense.)			
7. Misuse of sick leave such as working at another job without permission during any period of sick leave, or using sick leave for absences unrelated to illness or medical care (in which case the leave should be changed to AWOL in addition to appropriate disciplinary or failure to follow instructions for notifying the supervisor or obtaining approval for absence.	Warning notice to removal	Reprimand to removal	Removal
8. Insubordination: deliberate refusal to comply with authorized instructions issued by a supervisor, disrespect, insolence, and like behavior.	Reprimand to removal	Suspension to removal	Removal
9. Neglect of duty: sleeping on duty, loafing, deliberate failure to be at work on task assigned, unreasonable delay or failure in carrying out instructions, conducting personal affairs on official time, or careless workmanship resulting in waste or delay.			
a. Where safety of persons or property is not endangered.	Warning notice to reprimand	Reprimand to suspension	Removal
b. Where safety of persons or property is endangered.	Reprimand to removal	Removal	
10. Disorderly conduct.			
a. Use of abusive or offensive language, quarreling, creating a disturbance which adversely affects production or morale.	Warning notice to suspension	Reprimand to removal	Removal

Figure 3-112.1. Penalty Guide, Table 1
(Part 2 of 3)

Types of Delinquency or Misconduct	1st Offense	2nd Offense	3rd Offense
b. Fighting, threatening, attempting inflict or inflicting bodily injury to another individual.	Reprimand to removal	Suspension to removal	Removal
11. Violation of regulations where safety of persons or property is endangered (other than items 1 and 8, above).	Reprimand to removal	Suspension to removal	Removal
12. Indebtedness: failure to demonstrate conscientious effort to pay just financial obligations in a proper and timely manner, or to live up to arrangements agreed upon for payment. (Note: actions should be carefully evaluated for nexus to employment)	Warning notice	Reprimand	Reprimand to removal
13. Engaging in outside employment, business or professional activity without informing supervisor in writing and in advance.			
a. When no conflict of interest is involved	Warning notice	Reprimand	Reprimand to removal
b. When a conflict of interest is involved.	Reprimand to removal	Removal	
14. Unauthorized use of the Federal Telecommunications System or commercial or other official telecommunications facilities.	Warning notice	Reprimand	Reprimand to removal
15. Failure, through willfulness or with reckless disregard for the regulations, to observe any security regulation or order prescribed by competent authority.[1]			
a. Where the violation involved information classified Secret or above.	Reprimand to removal	Removal	
b. Where the violation involved information classified below Secret.	Reprimand to removal	Suspension to removal	Removal
16. Failure, through simple negligence or carelessness, to observe any security regulation or order prescribed by competent authority.	Reprimand to removal	Suspension to removal	Removal

[1] Investigations of security violations must be done initially by security managers in accordance with ADM P 1025.2B, ch. 10

Figure 1-112.1. Penalty Guide, Table I
(Part 3 of 3)

Types of Delinquency or Misconduct	1st Offense	2nd Offense	3rd Offense
1. Unauthorized use, removal, or possession of Government property, funds, services, supplies, or materials, including use or permitting the improper use of Government charge cards, Accounting Control Transaction (ACT) numbers or other obligating transaction devices, or the property of other employees. (In arriving at the penalty, consideration should be given to the value of the property involved and whether voluntary restitution was made.)	Suspension to removal	Removal	
2. Knowing and willful misstatement or omission of material facts from, unlawful concealment, removal, alteration, mutilation, or destruction of any official document, contract files, or records.	Reprimand to removal	Suspension to removal	Removal
3. Conduct as described in 2 above which results in: Accepting incomplete services, supplies, or materials or misrepresentation of contract inspections, etc., and/or false certification for work not performed or supplies, services, or materials not received; preparing or issuing a contract for services, supplies, or materials which exceeds reasonable requirements; requesting and accepting services, supplies, or materials other than those contracted for; and preparing an inaccurate Government estimate resulting in the acceptance of a given bid/price proposal from a contractor thereby causing damage or financial loss.	Suspension to removal	Removal	
4. Knowing and willful misappropriation of Government funds or other funds which come into employee's possession by reason of his official position.	Suspension to removal	Removal	

1 Contract throughout this penalty guide denotes all procurement actions which bind the Government, and includes purchase orders, leases and other contracted arrangements.

Figure 3-112.2. Penalty Guide, Table II (Part 1 of 5) Infractions that must be referred to the OIG

Types of Delinquency or Misconduct	1st Offense	2nd Offense	3rd Offense
5. Knowing and willful misstatement of one or more claims (travel vouchers, imprest fund vouchers, time and attendance records, etc.)[1]			
a. Claims for $100 or less.	Reprimand to removal	Removal	
b. Claims for more than $100.	Suspension to removal	Removal	
6. Partisan political activity in violation of the law.	Removal or other action as directed by OPM		
7. Knowing and willful use of public office for private gain.	Suspension to removal	Removal	
8. Misconduct whether or not in violation of a criminal statute, which impairs job performance or trustworthiness of the employee or otherwise affects the ability of a part of GSA to perform its mission.	Reprimand to Removal	Suspension to removal	Removal
9. Willful use or authorizing use of Government-owned or leased passenger motor vehicles or aircraft for unofficial purposes.	30 day Suspension to Removal[1]	Removal	
10. Loss of or damage to Government property:			
a. Through carelessness or negligence or when property involved is of small value.	Warning to suspension	Reprimand to suspension	Suspension to removal
b. Through maliciousness or intent, or when property involved is of significant value.	Reprimand to removal	Suspension to removal	Removal
11. Failure, through negligence, to account properly for Government funds.	Reprimand	Removal	
12. Negligent control of Accounting Control Transaction (ACT) numbers, Government charge cards, and other obligating forms and devices.	Reprimand to suspension	Suspension to removal	Removal

[1] A 30 day suspension is the minimum penalty prescribed by statute (31 USC 1349(b)). Where the element of willfulness is not clearly shown or when the vehicle is not a passenger vehicle, the same or lesser penalty may be imposed depending on the circumstances.

Figure 3-112.2. Penalty Guide, Table II
(Part 2 of 6) Infractions that must be referred to the OPC

Types of Delinquency or Misconduct	1st Offense	2nd Offense	3rd Offense
13. Failure to report to the Office of the Inspector General:			
a. Apparent or suspected violations of law in connection with an operation of GSA.	Reprimand to removal	Suspension to removal	Removal
b. Apparent or suspected violation of an order, regulation, or directive in connection with an operation of GSA.	Warning notice to removal	Reprimand to removal	Removal
14. Refusal to provide information in connection with an authorized investigation, and to furnish a signed statement when required, except where such refusal is based upon grounds of self-incrimination in potential criminal prosecution, or privileged communications.	Reprimand to removal	Suspension to removal	Removal
15. Negligent or willful mismanagement of a contract, or failure to administer provisions thereof, whether or not it results in a loss to the Government.	Reprimand to removal, with a minimum of suspension if the employee acted knowingly and willfully	Suspension to removal	Removal
16. Negligent or willful failure to maintain contract files in a complete and current manner in accordance with regulations and GSA requirements.	Reprimand to removal[3]	Suspension to removal	Removal
17. Knowing and willful failure to secure adequate and required competition for contracts in accordance with applicable regulations.	Suspension to removal	14 day suspension to removal	Removal
18. Awarding of more than one contract/purchase order with the intent of avoiding limitations on contracting authority or the requirements of applicable regulations.	Suspension to removal	14 day suspension to removal	Removal
19. Negligently or willfully awarding contracts which exceed contracting authority.	Reprimand to removal3	Suspension to removal	Removal

3 As in Item # 15.

Figure 9-112.4. Penalty Guide, Table II
(Part 3 of 5) Infractions that must be referred to the OIG

Types of Delinquency or Misconduct	1st Offense	2nd Offense	3rd Offense
20. Negligent or willful: (1) acceptance of incomplete services, supplies, or materials; or (2) misrepresentation of contract inspections and certification for work not performed or services, supplies, or materials not received.	Reprimand to removal[3]	Suspension to removal	Removal
21. Negligently or willfully preparing or issuing a doubtful for quantities which exceed reasonable requirements.	Reprimand to removal[3]	Suspension to removal	Removal
22. Negligently preparing an inaccurate Government estimate resulting in the acceptance of a given bid/price proposal from a contractor which thereby causes loss to the government.	Reprimand to suspension	Suspension to removal	Removal
23. Knowingly making false statements which are slanderous or defamatory about other employees or officials.	Reprimand to removal	Removal	
24. Gambling, betting, or promotion thereof on Government-owned or leased property, or while on duty for GSA.	Reprimand to removal	Suspension to removal	Removal
25. Soliciting or making a contribution for a gift (as defined by the GSA Standards of Conduct) to an official superior, or acceptance of such a gift by an official superior.	Removal[4]		
26. Gaming money for profit on Government-owned or leased premises to any other person; borrowing money from a subordinate or accepting a subordinate's endorsement on a loan.	Reprimand to removal	Removal	
27. Sale or possession of illegal drugs on Government-owned or leased premises or while on duty.	Suspension to removal	Removal	

[3] As in item # 15.

[4] Required by statute (5 USC 7352).

Figure 3-112.1. Penalty Guide, Table II
(Part 4 of 5) Infractions that must be referred to the OIG

Types of Delinquency or Misconduct	1st Offense	2nd Offense	3rd Offense
28. Unethical or improper use of official authority or credentials, or unauthorized disclosure or use of official information.	Reprimand to removal	Removal	
29. Improper solicitation or acceptance of gifts, loans gratuities, favors, etc., from persons, firms, or corporations with whom employees have official relations.	Reprimand to removal	Removal	
30. Violating GSA regulations prohibiting the purchase of Government property, personal or real, being sold by GSA.	Reprimand to removal	Removal	
31. Negligent or willful discrimination, including harassment against any employee or applicant for employment based on race, color, religion, sex, age, national origin, physical or mental handicap, marital status, or lawful political affiliation.	Warning notice to removal	Reprimand to removal	Removal
32. Reprisal action against any person for proper exercise of the right to file a discrimination complaint or grievance, or for reporting an irregularity, real or suspected.	Warning notice to removal	Reprimand to removal	Removal
33. Negligent or willful violation of GSA regulations regarding financial interests or transactions that conflict with the performance of official duties.	Warning notice to reprimand	Reprimand to removal	Removal

Figure 3-112.2. Penalty Guide, Table II
(Part 5 of 9) Infractions that must be referred to the OIG

Do not leave your assigned post for any reason unless you are properly relieved by a replacement guard or until the time the post hours end (depending on the post requirements). When you leave your post you must document on all records and logs that you are not on duty. The relief guard will sign in and work while you are on break. A supervisor cannot perform both as a productive guard and supervisor at the same time.

If you have any questions about any situation not covered in this Manual, contact your supervisor for directions or clarification.

The following is a list of grounds for disciplinary action, up to and including permanent removal from any GSA guard service contract:

1. Assault – making or uttering physical or verbal threats.
2. Arson.
3. Theft or pilferage.
4. Sabotage.
5. Willful or careless destruction of property, or vandalism.
6. Dishonesty – accepting bribes, enabling a person to secure stolen property, permitting unauthorized access to a facility or protected materials, or lying to a Government official or your supervisor.
7. Misuse of weapons, whether assigned to you or not.
8. Insubordination towards the visitors, your supervisor(s), or Government personnel.
9. Disregarding orders, including your Post Orders, special orders or instructions, or verbal instructions from your supervisor(s) or the Government's Contracting Officer's Representative.
10. Immoral conduct or any other criminal act that violates rules, regulations, or established policy of the Government.
11. Sexual harassment or discrimination towards visitors or Government employees.
12. Intoxication – being under the influence of any substance that impairs your ability to perform your duties, such as alcohol, illegal substances,

or medication with impairing side effects. Additionally, failing to pass illegal drug screening test.
13. Negligence – sleeping on duty, abandoning your post without being properly relieved, or failing to perform your duties as prescribed.
14. Absenteeism – failure to report for duty, or unsatisfactory attendance.
15. Tardiness – repeated failure to report to duty at the scheduled time.
16. Falsifying, concealing, removing, mutilating, damaging, or destroying official documents or records, or concealing important facts by leaving them out of official documents.
17. Reading, copying, removing, damaging, or destroying Government or proprietary business documents that you do not have access to during your normal course of duties.
18. Disorderly conduct – abusive or offensive language, quarreling, fighting, or attempting to intimidate someone. This also includes interfering with normal, efficient operations or performing your assigned duties.
19. Unethical or improper use of official authority, credentials, or equipment.
20. Unauthorized use of communications equipment (e.g., telephones, computers, radios) or other Government property.
21. Unreasonable delays or failure to complete job assignments; conducting personal business while on duty; refusing to assist someone as required in your Post Orders.
22. Failing to cooperate with Government officials, local law enforcement officials, or your employer during an official investigation.

2.6 Dealing With People

Success in security and law enforcement depends largely on the ability to deal with people effectively. Your success as a contract guard depends on how well you interact with people from all walks of life. People react to how you look, how you act, how you speak, and how you treat them. Even though you are not a Federal employee, you represent FPS as well as your employer. You are often the first contact the public has when entering a GSA-controlled facility and the last person they see when they leave. Visitors and employees will make immediate judgements about you based on your appearance, your demeanor, your body language, and your performance. These conclusions color their impression of the agency visited and the Government as a whole. The impression you make is a

8. **IMPORTANT NOTE:** Because the Certification card does not expire when individual certification elements expire, the Contractor is responsible for continually maintaining validity of each element of the Contract employee's certification status (i.e., suitability determination, medical examination, firearms requalification, CPR/First Aid certification). See Section J, Exhibit 11 for the list of individual certification elements.

9. **The CO shall have the express authority to demand return of the GSA Certification card for any Contract employee who does not maintain compliance with the Contract qualification and certification standards, and the CO shall have the express authority to prohibit that employee from performing under the Contract until such time as he/she comes into full compliance with all qualification/certification criteria.**

H-3 Identification/Building Pass

When a controlled personnel identification system is used by a tenant agency at a site at which the Contract employee is assigned for duty, the tenant agency will provide the Contract employee with the necessary Government identification. The Contractor shall ensure that all Government identifications are returned to the issuing agency when employees are terminated or resign, or upon expiration of the Contract, whichever comes first.

H-4 Standards of Conduct

1. The Contractor shall be responsible for maintaining satisfactory standards of employee competency, conduct, appearance, and integrity, and shall be responsible for taking such disciplinary action with respect to his employees as may be necessary.

2. The Contractor is also responsible for ensuring that their employees do not disturb papers on desks, open desk drawers or cabinets, or use Government telephones, except as authorized by this Contract and the post orders.

3. Each Contract employee is expected to adhere to standards of behavior that reflect credit on himself, his employer, and the Federal Government. The CO and COR have the authority to request the retraining, suspension, or removal of any Contract employee who does not meet and adhere to the standards of conduct as required in this Contract and the CGIM.

H-5 Removal from Duty

1. The Government may request the Contractor to immediately remove any employee from the work site should it be determined that the employee has been disqualified for either suitability or security reasons, or who is found to be unfit for performing security duties during his/her tour of duty. The

Contractor must comply with these requests in a timely manner. For clarification, a determination of unfitness may be made from, but not be limited to, incidents involving the most immediately identifiable types of misconduct or delinquency as set forth below:

A. Violations of the Rules and Regulations governing Public Buildings and Grounds, 41 CFR 101.20.3.
B. Neglect of duty, including sleeping while on duty, unreasonable delays or failure to carry out assigned tasks, conducting personal affairs during official time, and refusing to render assistance or cooperate in upholding the integrity of the security program at the worksite(s).
C. Falsification or unlawful concealment, removal, mutilation, or destruction of any official documents or records, or concealment of material facts by willful omissions from official documents or records.
D. Disorderly conduct, use of abusive or offensive language, quarreling, intimidation by words or actions, or fighting. Also, participating in disruptive activities which interfere with the normal and efficient operations of the Government.
E. Theft, vandalism, immoral conduct, or any criminal actions.
F. Selling, consuming, or being under the influence of intoxicants, drugs, or substances which produce similar effects; failure to pass drug screening test.
G. Improper use of official authority or credentials.
H. Unauthorized use of communications equipment or Government property.
I. Misuse of weapon(s).
J. Violation of security procedures or regulations.
K. Unauthorized post abandonment.
L. Failure to cooperate with Government officials or local law enforcement authorities during an official investigation.

2. The CO will make all determinations regarding the removal of any employee from the work site. In the event of a dispute, the CO will make the final determination. Specific reasons for removal of an employee will be provided to the Contractor in writing.

H-6 Contract Employee Reinstatements

1. When an action is taken by the Government that may impact upon the suitability or work fitness status of a Contract employee, the Contractor may appeal the decision to the CO.

2. If the CO made the initial decision, the appeal will be reviewed by a senior manager within the regional FPS office or by the FPS Technology and Security Branch staff in Washington, DC. The appeal decision will be provided to the Contractor in writing with a brief explanation of the decision to

SECTION J, EXHIBIT 4

TRAINING SUBJECTS TO BE PRESENTED TO THE CONTRACT GUARDS BY THE CONTRACTOR

IMPORTANT NOTE: THE INSTRUCTOR IS STRONGLY ENCOURAGED TO USE THE FPS CONTRACT GUARD INFORMATION MANUAL (CGIM) AS AN ESSENTIAL COMPONENT OF THIS TRAINING. TOPICS ARE CROSS REFERENCED WHERE APPLICABLE TO THE MANUAL FOR EFFECTIVE PRESENTATION OF THE MATERIAL.

72 Hours[1]

Subject	Hours	Scope
Overview of the General Services Administration and the Federal Protective Service (CHAPTER ONE, CGIM)	2	Instructor(s) will discuss the mission, role, and responsibilities of GSA and FPS as well as the role contract guards play in facility security. Instructor will also discuss the five types of facilities and security levels
Customer Oriented Protection	2	Instructor(s) will discuss the concept of Customer Oriented Protection and the Role contract guards play in this approach to security *(Note: GSA will provide the t instructor with information on this program to assist in training)*
Overview of the Roles & Responsibilities of a Contract Guard (CHAPTER TWO, CGIM)	2	Instructor will discuss the typical duties and responsibilities associated with being a contract guard at a federal facility;
Ethics and Professionalism Part I: Overview (CHAPTER TWO, CGIM)	1	Describe police professionalism today, including the expanding use of contract guards and indicate by current trends where it may be headed in the future. Provide instruction in police ethics, using practical examples, both desirable and undesirable. Discuss ideas that will lead to improved cooperation between the local, state, and Federal law enforcement guards and the contract guards.

[1] The Contractor must present 72 hours of basic training to all students. The hours listed in the "Hours" column are the recommended times needed for effective coverage of the material, to include questions and answers, interactive tasks, and reviews/quizzes of the material. The Instructor shall use his/her expertise in evaluating the class's progress in comprehending and applying the concepts and materials taught. There may be some fluctuation in the actual time covered for each subject, *but under no circumstances shall the Instructor provide less than 72 hours of training.* It is also incumbent upon the instructor to notify the Contractor of instances where students are not adequately mastering the subject matter or are presenting a disruption to the class by repeated lateness, absences, or disrespectful behavior such as sleeping or talking while instruction is being given. Such behavior indicates that the student may not be suitable for holding a position as a security guard at a federal facility.

SECTION J, EXHIBIT 4, continued

Subject	Hours	Scope
Ethics and Professionalism Part II: Interactive Training	1	Role playing or other interactive methods between instructor and students using scenarios of ethical and Professional behavior by guards based on the overview of this topic. Use of audio-visual materials, case studies, and other materials to facilitate training objectives will be acceptable.
Principles of Communications Part I: Overview (CHAPTER TWO, CGIM)	2	Familiarize the contract guards with the concept surrounding effective communications and development of communication skills. In meeting this objective, the contract guard is presented with the theory of communications; various types of obstacles which can hinder the development and maintenance of effective communication; the senses and their role in the communication process and the main and essential skills which accompany the development of communication effectiveness.
Principles of Communications Part II: Interactive Training	1	Role playing or other interactive methods between instructor and students using scenarios of communication methods based on the overview of this topic. Use of audio-visual materials, case studies, and other materials to facilitate training objectives will be acceptable.
Professional Public Relations Part I: Overview (CHAPTER TWO, CGIM)	1	Instruction is to be provided to the contract guards which will increase their effectiveness in the use of basic social skills, enhance their employer's reputation and contract performance as well as the positive image portrayed by the U.S. Government. Such instruction should include (but not be limited to) proper display of the uniform, shoeshine, haircuts, and other forms of personal grooming.
Professional Public Relations Part II: Interactive Training	1	Role playing or other interactive methods between instructor and students using Scenarios of communication methods based on the overview of this topic. Use of audio-visual materials, case studies, and other materials to facilitate training objectives will be acceptable.

SECTION J, EXHIBIT 4, continued

Subject	Hours	Scope
Understanding Human Behavior, Part I: Overview (CHAPTERS TWO AND NINE, CGIM)	1	Instructor(s) will discuss the basic knowledge needed for the contract guards to understand their own actions, and those of the people they work with in the performance of their assigned duties. Behavior under stress (both natural and man induced); actions of mentally disturbed; irrational conduct created by the use of drugs or alcohol; job (performance) related problem; will be a part of this discussion. Special attention should be given to the changes in human behavior that might occur in the contract guard with the introduction of badge and gun.
Understanding Human Behavior, Part II: Interactive Training	1	Role playing or other interactive methods between instructor and students using scenarios of human behavior based on the overview of this topic. Use of audio-visual materials, case studies, and other materials to facilitate training objectives will be acceptable.
The Law, Legal Authorities, Jurisdiction and Responsibilities (CHAPTER THREE, CGIM)	2	Discuss history of laws, applicable laws and regulations, and the concept of legal jurisdiction as it pertains to the guards' duties and authority.
Crimes and Offenses (CHAPTER THREE, CGIM)	1	Present the contract guards with an understanding of the types of offenses they are most likely to encounter in their duties. Instruction should be given in methods of successful investigative techniques.
Search and Seizure (CHAPTER THREE, CGIM)	1	Provide the guard with the knowledge of the legal application of search and seizure law in the performance of duties as a contract guard with a Federal facility. Instruction should provide a comprehensive survey of laws pertaining to search and seizure to include "Stop and Frisk".

SECTION J, EXHIBIT 4, continued

Subject	Hours	Scope
Arrest Authority and Procedures (CHAPTER THREE, CGIM)	1	Provide the contract guard with knowledge of how guards shall exercise their arrest powers to the degree authorized by local, state, and Federal regulations. Instruction will define arrest procedures and legal rules governing practices and procedures: arrest, interrogations and confessions, self incrimination privilege, entrapment, eyewitness identifications and complaints and warrants. Contract guards should become completely familiar with the extent of their arrest powers obtained from the various jurisdictions involved.
Use of Force (CHAPTER THREE, CGIM)	1	Instruction will be given on the use of force, to include the various degrees of force authorized in the performance of duties under this contract. Reporting procedures related to such use will be discussed as will the consequences of the unauthorized, or misuse, of force.
Crime Scene Protection (CHAPTER THREE, CGIM)	1	Illustrate the important facets of the preliminary investigation and the protection, preservation, and subsequent search of the crime scene.
Rules of Evidence (CHAPTER THREE, CGIM)	1	Evidence is defined to include direct, circumstantial and real. Information will be provided on admissibility as it relates to competency, relevancy, materiality, and hearsay. Instructions will present information on the exclusionary rule and other related items. Instructor will discuss procedures for handling and protecting evidence.
Contract Guard Administration (CHAPTER FOUR, CGIM)	1	Instructor(s) will discuss the relationship between the Contractor and the Government And will discuss protocol for communicating with the Control Centers when incidents occur. Instructor will also discuss the Importance of the Duty Book.
Post Duties (CHAPTER FOUR, CGIM)	1	Instructor(s) will discuss the purpose of posts and identify the various types of protective services. Discuss the necessity of proper observation and counter-surveillance while manning a post

SECTION J, EXHIBIT 4, continued

Subject	Hours	Scope
Patrol Methods And Patrol Hazards (CHAPTER FOUR, CGIM)	1	Study the various methods and skills employed in protective patrols. Explain the importance of patrol to law enforcement and explore the values of various patrol methods. Examine the hazards encountered during patrol functions, both natural and man made. Discuss the techniques or recognition and ways to eliminate, or reduce patrol hazards.
General Response Procedures (CHAPTER FOUR, CGIM)	1	Explain the various types of situations guards will respond to. Describe the proper approach to such situations; discuss the guard's role and responsibility; and instruct in the appropriate techniques to be employed in such circumstances. Include discussion of radio communications protocol.
Access Control (CHAPTER FIVE, CGIM)	2	Describe importance of proper access control of protected space. Discussion shall include personnel control, property control, vehicle control, and lock and key control.
Crime Detection, Assessment And Response (CHAPTER SIX, CGIM)	2	Acquaint the contract guard with the care and caution that must be exercised when coming upon a crime in progress. Discuss the element of surprise, and the possibilities of encountering a crime being committed. Special emphasis should be placed on the crimes the contract guard may encounter while on duty within a Federal facility, his actions, responses, and the requirements of the agency.
Safety and Fire Prevention (CHAPTER SEVEN, CGIM)	1	Define the contract guard's responsibility for safety and fire prevention. Provide guidelines for operational safeguards including the use of fire extinguishers (types, etc.), sprinkler systems, fire alarm systems, and other standard fire prevention equipment.
Records and Reports (CHAPTER EIGHT, CGIM)	3	Instructor will lecture on importance of Properly prepared records and reports. Students shall be given examples and prepare sample records and reports as they will use on a GSA contract. Emphasis on tips for effective report writing.

SECTION J, EXHIBIT 4, continued

Subject	Hours	Scope
Special Situations (CHAPTER NINE, CGIM)	2	Instructor shall discuss various types of special situations which guards may be required to respond to, such as providing escorts; controlling traffic; and dealing with mentally ill or disturbed persons.
Emergency First Aid and Bloodborne Pathogens (CHAPTER TEN, CGIM)	3	Instructor will provide instruction on the necessary skills to deal with hazards of exposure to bloodborne pathogens as follows: Explanation of the bloodborne pathogens standard; how bloodborne diseases can be transmitted; exposure control plan for incidents regarding bloodborne diseases; employee hazard recognition; and ways to prevent the exposure. Instructor will also discuss procedures to follow for emergencies. (Note: this training is not a substitute for First Aid training, which must be provided an the American Red Cross accredited instructor. Guards must receive at least 9 hours of Red Cross certified First Aid and CPR training.)
Flying the Flag (CHAPTER ELEVEN, CGIM)	1	Instructor will discuss where and when the American flag is flown and will give hands-on demonstration for folding and storing the flag.
Terrorism, Anti-terrorism, & Weapons of Mass Destruction (WMD) (CHAPTER TWELVE, CGIM)	2	Instructor will provide a lecture regarding domestic and international terrorism and weapons of mass destruction; discuss anti-terrorism methods used by FPS such as counter-surveillance and proper use of building security equipment
Workplace Violence (CHAPTER THIRTEEN, CGIM)	2	Instructor will discuss workplace violence; Who commits violent acts and why; guard Response to violent incidents, and tactics For being aware of environments or Situations that can contribute to violence.
Civil Disturbances (CHAPTER FOURTEEN, CGIM)	2	Instructor (s) will discuss and provide field practice in crowd control and will teach the guards how to distinguish between friendly, sightseeing, agitated, and hostile crowds.. Emphasis shall be placed upon effective response to civil disturbances.

SECTION J, EXHIBIT 4, continued

Subject	Hours	Scope
Bomb Threats and Incidents (CHAPTER FIFTEEN, CGIM)	2	Instructor(s) will discuss the procedures guards will use to respond to bomb threats, discovery of suspicious items and persons who appear t o be suspicious. Emphasis shall be placed on gathering as much information as possible and reportiing incidents.
Hostage Situations (CHAPTER SIXTEEN, CGIM)	2	Lecture and practical applications to instruct guards on identifying and responding to hostage situations.
Sabotage and Espionage (CHAPTER SEVENTEEN, CGIM)	2	Instructor will lecture on defining the terms and give concrete examples of the concepts as they might occur on federal property. Emphasize importance of deterrence and prevention, then response to incidents as they occur.
Defensive Tactics	4	Lecture and practical applications will be used to instruct Security Guards in the use of defensive tactics. Instructor will incorporate defense against armed and unarmed attack, restraining hold, and subjective compliance methods against hostile or uncooperative persons.
Use of Handcuffs	4	Lecture and hands-on demonstrations of procedures and techniques for handcuffing persons. All students shall be given the opportunity to affix and remove handcuffs in different "real life" scenarios where handcuffing would be necessary.
Use of Expandable Baton	8	Lecture and hands-on demonstration of procedures for baton carrying and drawing as well as striking techniques.
Firearms Safety, Handling	1	(NOTE: This segment does not include fundamentals or firing and firearms qualification.) Provide instruction in the handling and control of the contract guard's firearm. Instruction should relate to weapons safety and handling to include nomenclature, wearing of the weapon, care and cleaning, storage and accountability. Special emphasis must be placed on loading, unloading and the safe lowering of a "cocked" hammer on a live round.

SECTION J, EXHIBIT 4, continued

Subject	Hours	Scope
Review & Examination	2	A 50 question multiple-choice written examination will be given to determine knowledge and understanding of the academic subject matter.

NOTE: THE WRITTEN EXAMINATION QUESTIONS ARE TAKEN 100% FROM THE CGIM. FAILURE BY THE INSTRUCTOR TO USE THE CGIM AS AN ESSENTIAL TRAINING TOOL MAY RESULT IN HIGH RATES OF FAILURE ON THE WRITTEN EXAMINATION. THE CONTRACTOR IS STRONGLY URGED TO ENSURE THAT THE INSTRUCTORS USE THE CGIM AS A CORE COMPONENT OF THE TRAINING.

SECTION J, EXHIBIT 5

SUPERVISORY TRAINING SUBJECTS TO BE PRESENTED BY THE CONTRACTOR

9 Hours

Subject	Hours	Scope
Supervisor's Duties and Responsibilities	2	Instructor(s) will discuss the basic duties and responsibilities of a GSA Contract Guard supervisor. Discussions will include instructions that all duty posts are to be manned at all times as required by the Contract; that all required GSA forms are to be completed in an accurate, legible and timely manner; and that all subordinate employees have all required equipment and maintain proper inventory records of service weapons and all other required equipment.
GSA Contract Requirements	1	Instructor(s) will review basic GSA Contract requirements and standards of performance for Contractors, Contract employees, and the relationship of employees with key members of Government agencies and GSA officials involved in the administration and operation of GSA Contracts. An actual Contract will be discussed so that students will be familiar with all aspects of such Contracts to ensure proper performance by all employees and supervisors.
Methods and Theories of Supervision	1	Instructor(s) will discuss various management theories and the basic principles involved so that the student understands the various methods of supervision that are available to accomplish the goals of a first-line supervisor.
How to be an Effective Leader	1	Instructor(s) will discuss the importance of a supervisor being a good leader. Discussion will focus on the necessity of giving constant attention to countless details of personal behavior and personal relations with subordinates.

SECTION J, EXHIBIT 5, Continued

SUPERVISORY TRAINING SUBJECTS TO BE PRESENTED BY THE CONTRACTOR

Subject	Hours	Scope
Purpose of Discipline	1	Instructor(s) will discuss the purpose of discipline and the use of praise and criticism to encourage and motivate employees. Discussion will focus on the use of criticism with the intention of improving job performance.
Effective Written and Oral Communication	1	Instructor(s) will discuss the problems encountered in both written and oral communication between supervisors and subordinates and methods to improve both. Lecture will include discussion of quantitative directives and the concept of asking while telling. Also included will be information on formal and informal communications and how the effective supervisor can use both to accomplish his/her mission as a first-line supervisor.
Motivating Employees and Problem Solving Methods	1	Instructor(s) will discuss methods used to motivate employees and to improve the performance of those employees who are not performing at acceptable standards. Emphasis will be on early identification of problem employees and methods that may be used to bring poor performance up to acceptable standards. Discussion will include problems related to alcoholism, illegal drug usage, and other related topics.
Scheduling Employees	1	Instructor(s) will discuss scheduling problems and methods to use available personnel effectively to ensure coverage of all posts in a cost-effective manner without using overtime. Included will be several practical "hands on" scheduling exercises.

SECTION J, EXHIBIT 6

CONTRACTOR PROVIDED RECERTIFICATION TRAINING TO BE PRESENTED TO ALL CONTRACT GUARDS

40 Hours

Subject	Hours	Scope
Overview of the General Services Administration and the Federal Protective Service (CHAPTER ONE, CGIM)	1	Instructor(s) will discuss the mission, role, and responsibilities of GSA and FPS as well as the role contract guards play in facility security. Instructor will also discuss the five types of facilities and security levels
Customer Oriented Protection	1	Instructor(s) will discuss the concept of Customer Oriented Protection and the Role contract guards play in this approach to security *(Note: GSA will provide the t instructor with information on this program to assist in training)*
Overview of the Roles & Responsibilities of a Contract Guard (CHAPTER TWO, CGIM)	1	Instructor will discuss the typical duties and responsibilities associated with being a contract guard at a federal facility;
Ethics and Professionalism Part I: Overview (CHAPTER TWO, CGIM)	1	Describe police professionalism today, including the expanding use of contract guards and indicate by current trends where it may be headed in the future. Provide instruction in police ethics, using practical examples, both desirable and undesirable. Discuss ideas that will lead to improved cooperation between the local, state, Federal law enforcement guards, and the contract guards.

[1] The Contractor must present 40 hours of re-certification training to all students. The hours listed in the "Hours" column are the recommended times needed for effective coverage of the material, to include questions and answers, interactive tasks, and reviews/quizzes of the material. The Instructor shall use his/her expertise in evaluating the class's progress in comprehending and applying the concepts and materials taught. There may be some fluctuation in the actual time covered for each subject, *but under no circumstances shall the Instructor provide less than 40 hours of training.* It is also incumbent upon the instructor to notify the Contractor of instances where students are not adequately mastering the subject matter or are presenting a disruption to the class by repeated lateness, absences, or disrespectful behavior such as sleeping or talking while instruction is being given. Such behavior indicates that the student may not be suitable for holding a position as a security guard at a federal facility.

SECTION J, EXHIBIT 6, continued

Subject	Hours	Scope
Ethics and Professionalism Part II: Interactive Training	1	Role playing or other interactive methods between instructor and students using scenarios of ethical and Professional behavior by guards based on the overview of this topic. Use of audio-visual materials, case studies, and other materials to facilitate training objectives will be acceptable.
Principles of Communications Part I: Overview (CHAPTER TWO, CGIM)	1	Familiarize the contract guards with the concept surrounding effective communications and development of communication skills. In meeting this objective, the contract guard is presented with the theory of communications; various types of obstacles which can hinder the development and maintenance of effective communication; the senses and their role in the communication process and the main and essential skills which accompany the development of communication effectiveness.
Principles of Communications Part II: Interactive Training	1	Role playing or other interactive methods between instructor and students using scenarios of communication methods based on the overview of this topic. Use of audio-visual materials, case studies, and other materials to facilitate training objectives will be acceptable.
Professional Public Relations Part I: Overview (CHAPTER TWO, CGIM)	1	Instruction is to be provided to the contract guards which will increase their effectiveness in the use of basic social skills, enhance their employer's reputation and contract performance as well as the positive image portrayed by the U.S. Government. Such instruction should include (but not be limited to) proper display of the uniform, shoeshine, haircuts, and other forms of personal grooming.
Professional Public Relations Part II: Interactive Training	1	Role playing or other interactive methods between instructor and students using Scenarios of communication methods based on the overview of this topic. Use of audio-visual materials, case studies, and other materials to facilitate training objectives will be acceptable.

SECTION J, EXHIBIT 6, continued

Subject	Hours	Scope
Understanding Human Behavior, Part I: Overview (CHAPTERS TWO AND NINE, CGIM)	1	Instructor(s) will discuss the basic knowledge needed for the contract guards to understand their own actions, and those of the people they work with in the performance of their assigned duties. Behavior under stress (both natural and man induced); actions of mentally disturbed; irrational conduct created by the use of drugs or alcohol; job (performance) related problem; will be a part of this discussion. Special attention should be given to the changes in human behavior that might occur in the contract guard with the introduction of badge and gun.
Understanding Human Behavior, Part II: Interactive Training	1	Role playing or other interactive methods between instructor and students using scenarios of human behavior based on the overview of this topic. Use of audio-visual materials, case studies, and other materials to facilitate training objectives will be acceptable.
The Law, Legal Authorities, Jurisdiction and Responsibilities (CHAPTER THREE, CGIM)	1	Discuss history of laws, applicable laws and regulations, and the concept of legal jurisdiction as it pertains to the guards' duties and authority.
Crimes and Offenses (CHAPTER THREE, CGIM)	.5	Present the contract guards with an understanding of the types of offenses they are most likely to encounter in their duties. Instruction should be given in methods of successful investigative techniques.
Search and Seizure (CHAPTER THREE, CGIM)	.5	Provide the guard with the knowledge of the legal application of search and seizure law in the performance of duties as a contract guard with a Federal facility. Instruction should provide a comprehensive survey of laws pertaining to search and seizure to include "Stop and Frisk".

SECTION J, EXHIBIT 6, continued

Subject	Hours	Scope
Arrest Authority and Procedures (CHAPTER THREE, CGIM)	.5	Provide the contract guard with knowledge of how guards shall exercise their arrest powers to the degree authorized by local, state, and Federal regulations. Instruction will define arrest procedures and legal rules governing practices and procedures: arrest, interrogations and confessions, self incrimination privilege, entrapment, eyewitness identifications and complaints and warrants. Contract guards should become completely familiar with the extent of their arrest powers obtained from the various jurisdictions involved.
Use of Force (CHAPTER THREE, CGIM)	.5	Instruction will be given on the use of force, to include the various degrees of force authorized in the performance of duties under this contract. Reporting procedures related to such use will be discussed as will the consequences of the unauthorized, or misuse, of force.
Crime Scene Protection (CHAPTER THREE, CGIM)	.5	Illustrate the important facets of the preliminary investigation and the protection, preservation, and subsequent search of the crime scene.
Rules of Evidence (CHAPTER THREE, CGIM)	.5	Evidence is defined to include direct, circumstantial and real. Information will be provided on admissibility as it relates to competency, relevancy, materiality, and hearsay. Instructions will present information on the exclusionary rule and other related items. Instructor will discuss procedures for handling and protecting evidence.
Contract Guard Administration (CHAPTER FOUR, CGIM)	.5	Instructor(s) will discuss the relationship between the Contractor and the Government And will discuss protocol for communicating with the Control Centers when incidents occur. Instructor will also discuss the importance of the Duty Book.
Post Duties (CHAPTER FOUR, CGIM)	.5	Instructor(s) will discuss the purpose of posts and identify the various types of protective services. Discuss the necessity of proper observation and counter-surveillance while manning a post

SECTION J, EXHIBIT 6, continued

Subject	Hours	Scope
Patrol Methods And Patrol Hazards (CHAPTER FOUR, CGIM)	.5	Study the various methods and skills employed in protective patrols. Explain the importance of patrol to law enforcement and explore the values of various patrol methods. Examine the hazards encountered during patrol functions, both natural and man made. Discuss the techniques or recognition and ways to eliminate, or reduce patrol hazards.
General Response Procedures (CHAPTER FOUR, CGIM)	.5	Explain the various types of situations guards will respond to. Describe the proper approach to such situations; discuss the guard's role and responsibility; and instruct in the appropriate techniques to be employed in such circumstances. Include discussion of radio communications protocol.
Access Control (CHAPTER FIVE, CGIM)	.5	Describe importance of proper access control of protected space. Discussion shall include personnel control, property control, vehicle control, and lock and key control.
Crime Detection, Assessment And Response (CHAPTER SIX, CGIM)	.5	Acquaint the contract guard with the care and caution that must be exercised when coming upon a crime in progress. Discuss the element of surprise, and the possibilities of encountering a crime being committed. Special emphasis should be placed on the crimes the contract guard may encounter while on duty within a Federal facility, his actions, responses, and the requirements of the agency.
Safety and Fire Prevention (CHAPTER SEVEN, CGIM)	.5	Define the contract guard's responsibility for safety and fire prevention. Provide guidelines for operational safeguards including the use of fire extinguishers (types, etc.), sprinkler systems, fire alarm systems, and other standard fire prevention equipment.
Records and Reports (CHAPTER EIGHT, CGIM)	1	Instructor will lecture on importance of Properly prepared records and reports. Students shall be given examples and prepare sample records and reports as they will use on a GSA contract. Emphasis on tips for effective report writing.

SECTION J, EXHIBIT 6, continued

Subject	Hours	Scope
Special Situations (CHAPTER NINE, CGIM)	1	Instructor shall discuss various types of special situations which guards may be required to respond to, such as providing escorts; controlling traffic; and dealing with mentally ill or disturbed persons.
Emergency First Aid and Bloodborne Pathogens (CHAPTER TEN, CGIM)	1	Instructor will provide instruction on the necessary skills to deal with hazards of exposure to bloodborne pathogens as follows: Explanation of the bloodborne pathogens standard; how bloodborne diseases can be transmitted; exposure control plan for incidents regarding bloodborne diseases; employee hazard recognition; and ways to prevent the exposure. Instructor will also discuss procedures to follow for emergencies. (Note: this training is not a substitute for First Aid training, which must be provided an the American Red Cross accredited instructor. Guards must receive at least 9 hours of Red Cross certified First Aid and CPR training.)
Flying the Flag (CHAPTER ELEVEN, CGIM)	.5	Instructor will discuss where and when the American flag is flown and will give hands-on demonstration for folding and storing the flag.
Terrorism, Anti-terrorism, & Weapons of Mass Destruction (WMD) (CHAPTER TWELVE, CGIM)	1	Instructor will provide a lecture regarding domestic and international terrorism and weapons of mass destruction; discuss anti-terrorism methods used by FPS such as counter-surveillance and proper use of building security equipment
Workplace Violence (CHAPTER THIRTEEN, CGIM)	1	Instructor will discuss workplace violence; Who commits violent acts and why; guard Response to violent incidents, and tactics For being aware of environments or Situations that can contribute to violence.
Civil Disturbances (CHAPTER FOURTEEN, CGIM)	1	Instructor (s) will discuss and provide field practice in crowd control and will teach the guards how to distinguish between friendly, sightseeing, agitated, and hostile crowds.. Emphasis shall be placed upon effective response to civil disturbances.

SECTION J, EXHIBIT 6, continued

Subject	Hours	Scope
Bomb Threats and Incidents (CHAPTER FIFTEEN, CGIM)	1	Instructor(s) will discuss the procedures guards will use to respond to bomb threats, discovery of suspicious items and persons who appear t o be suspicious. Emphasis shall be placed on gathering as much information as possible and reportiing incidents.
Hostage Situations (CHAPTER SIXTEEN, CGIM)	1	Lecture and practical applications to instruct guards on identifying and responding to hostage situations.
Sabotage and Esplonage (CHAPTER SEVENTEEN, CGIM)	1	Instructor will lecture on defining the terms and give concrete examples of the concepts as they might occur on federal property. Emphasize importance of deterrence and prevention, then response to incidents as they occur.
Defensive Tactics	1	Lecture and practical applications will be used to instruct Security Guards in the use of defensive tactics. Instructor will incorporate defense against armed and unarmed attack, restraining hold, and subjective compliance methods against hostile or uncooperative persons.
Use of Handcuffs	2	Lecture and hands-on demonstrations of procedures and techniques for handcuffing persons. All students shall be given the opportunity to affix and remove handcuffs in different "real life" scenarios where handcuffing would be necessary.
Use of Expandable Baton	8	Lecture and hands-on demonstration of procedures for baton carrying and drawing as well as striking techniques.
Firearms Safety, Handling	1	(NOTE: This segment does not include fundamentals or firing and firearms qualification.) Provide detailed instruction in the handling and control of the contract guard's firearm. Instruction should relate to weapons safety and handling to include nomenclature, wearing of the weapon, care and cleaning, storage and accountability. Special emphasis must be placed on loading, unloading and the safe lowering of a "cocked" hammer on a live round.