SPEAKERS CONTENTS INSERTS

Page 1 TOP OF DOC

65–870

2000

BREACHES OF SECURITY AT FEDERAL AGENCIES AND AIRPORTS

HEARING

BEFORE THE

SUBCOMMITTEE ON CRIME

OF THE
COMMITTEE ON THE JUDICIARY
HOUSE OF REPRESENTATIVES

ONE HUNDRED SIXTH CONGRESS

SECOND SESSION

MAY 25, 2000

Serial No. 95

Printed for the use of the Committee on the Judiciary

Page 2 PREV PAGE TOP OF DOC

For sale by the U.S. Government Printing Office
Superintendent of Documents, Congressional Sales Office, Washington, DC 20402

JAMES E. ROGAN, California
LINDSEY O. GRAHAM, South Carolina
MARY BONO, California
SPENCER BACHUS, Alabama
JOE SCARBOROUGH, Florida
DAVID VITTER, Louisiana

Page 3 PREV PAGE TOP OF DOC

JOHN CONYERS, Jr., Michigan
BARNEY FRANK, Massachusetts
HOWARD L. BERMAN, California
RICK BOUCHER, Virginia
JERROLD NADLER, New York
ROBERT C. SCOTT, Virginia
MELVIN L. WATT, North Carolina
ZOE LOFGREN, California
SHEILA JACKSON LEE, Texas
MAXINE WATERS, California
MARTIN T. MEEHAN, Massachusetts
WILLIAM D. DELAHUNT, Massachusetts
ROBERT WEXLER, Florida
STEVEN R. ROTHMAN, New Jersey
TAMMY BALDWIN, Wisconsin
ANTHONY D. WEINER, New York

THOMAS E. MOONEY, SR., *General Counsel-Chief of Staff*
JULIAN EPSTEIN, *Minority Chief Counsel and Staff Director*

Subcommittee on Crime
BILL McCOLLUM, Florida, *Chairman*
STEVE CHABOT, Ohio
BOB BARR, Georgia

Page 4 PREV PAGE TOP OF DOC

GEORGE W. GEKAS, Pennsylvania
HOWARD COBLE, North Carolina
LAMAR S. SMITH, Texas
CHARLES T. CANADY, Florida
ASA HUTCHINSON, Arkansas

ROBERT C. SCOTT, Virginia
MARTIN T. MEEHAN, Massachusetts
STEVEN R. ROTHMAN, New Jersey
ANTHONY D. WEINER, New York
SHEILA JACKSON LEE, Texas

GLENN R. SCHMITT, *Chief Counsel*

DANIEL J. BRYANT, *Chief Counsel*
RICK FILKINS, *Counsel*
CARL THORSEN, *Counsel*
BOBBY VASSAR, *Minority Counsel*

C O N T E N T S

BREACHES OF SECURITY AT FEDERAL AGENCIES AND AIRPORTS

THURSDAY, MAY 25, 2000

House of Representatives,
Subcommittee on Crime,

Page 6 PREV PAGE TOP OF DOC

Committee on the Judiciary,
Washington, DC.

The subcommittee met, pursuant to call, at 2:13 p.m., in room 2141, Rayburn House Office Building, Honorable Bill McCollum [chairman of the subcommittee] presiding.

Present: Representatives Bill McCollum, George W. Gekas, Steve Chabot, Bob Barr, Asa Hutchinson, Robert C. Scott, Sheila Jackson Lee, and Henry J. Hyde [ex officio].

Staff Present: Daniel J. Bryant, Chief Counsel; Rick Filkins, Counsel; Veronica L. Eligan, Staff Assistant; and Bobby Vassar, Minority Counsel.

OPENING STATEMENT OF CHAIRMAN McCOLLUM

Mr. **MCCOLLUM.** This hearing of the Subcommittee on Crime will come to order.

Good afternoon. Today's hearing provides a timely opportunity for Congress to examine just how secure or insecure our agencies and buildings really are. We will also have a chance to look at how easily available bogus police badges are, and how they can be put to dangerous use to penetrate secure Federal agencies and our airports, and other buildings for that matter.

For some time I have been concerned with the fact that stolen and counterfeit police badges are readily available on the Internet and from other commercial sources, and that they can be used by criminals, terrorists, and foreign intelligence agents for illegal purposes, including penetrating our Nation's most secure government buildings, airports, and other facilities. Legislation addressing this concern is currently pending before this subcommittee.

Page 7 PREV PAGE TOP OF DOC

With this in mind, 7 weeks ago I requested that the General Accounting Office investigate the potential security risk to secure Federal facilities posed by the use of such badges. During the investigation that ensued, undercover OSI special agents targeted 19 secure Federal buildings and two major airports posing as plain-clothes law enforcement officers. In every case these agents were able to enter agency buildings while claiming to be armed and carrying briefcases, which were never searched, and were big enough to be packed with large quantities of explosives, chemicals, or biological agents.

The agencies penetrated included the CIA, the Pentagon, the FBI, the Justice Department, the State Department, and the Department of Energy. The agents were simply waved around the metal detectors. In many cases, they had the run of the buildings once they were inside, including the offices of department secretaries.

The agents drove a rental van into the courtyard of Main Justice without the van being inspected or searched. The van was parked in the courtyard and the agents left it while they went inside the building. On a single day, they succeeded in penetrating eight secure buildings. The havoc that could have been wreaked by terrorists during this same period of time is chilling, if you think about it—eight in one day.

For the two airports whose security was compromised, agents obtained boarding passes and foreign permits to carry weapons aboard flights for which they had purchased tickets. Like the Federal buildings they entered, they carried briefcases that were never x-rayed. They walked right up to the door that led down the gangway to the airplane. Nothing stood between them and the aircraft. They had fooled everyone.

Page 8 PREV PAGE TOP OF DOC

The agents' method was simple. They entered these buildings by flashing fake law enforcement badges and credentials and passing themselves off as Federal agents or local police officers. They assembled their bogus credentials by buying badges on the Internet and other sources and by using off-the-shelf computer graphics programs to generate official-looking identification cards. They then placed the badges and credentials in small leather cases and went to work.

To the untrained eye, these fake badges and credentials looked like the real thing. They were not perfect counterfeits by any means. They were not intended to be perfect copies of the real thing. And that fact alone is very disturbing.

What these agents did, a lot of people could do. Certainly members of a foreign intelligence service or a terrorist

organization could do it. I must say that I find the easy availability of these badges to be disconcerting. In fact, if you were to get on-line right now and go to eBay.com, you could find more than 600 police badges available for sale. There are dozens of other web sites where badges can be purchased.

Earlier this week, I held a closed-door briefing with my colleague, Mr. Scott, for the agencies whose security had been compromised in order to make known the details of how their buildings and airport security had been penetrated. At that briefing, preliminary recommendations were presented on how to immediately close these gaping security loopholes. And I am pleased to report that steps have already begun to be taken by some of these agencies—I hope all of these agencies—to address the problem.

Page 9 PREV PAGE TOP OF DOC

As we will hear from our witnesses in a moment, many of the recommendations are neither complicated nor expensive. They are really just common sense. What concerns me most about this investigation is that the undercover investigators were 19 for 19 with the agencies they targeted and two for two with the airports targeted. These findings point to a system-wide breakdown that is simply unacceptable.

This week we are having major counter-terrorism exercises in Washington, DC involving a wide range of sophisticated simulated terrorist attacks. That is all well and good, but these efforts to detect and prevent terrorist attacks cannot overlook the obvious: our secure buildings must have minimal security safeguards in place. Roaming around the halls of secured buildings unescorted and into cabinet members' offices with unchecked briefcases just doesn't cut it.

The bottom line is that we have learned that far too many of our secure facilities, where top secret and sensitive information is kept, have an open-door policy. As of this week, that is beginning to change.

I do want to say at the outset that the testimony presented today will be limited in certain important aspects so as to avoid providing a road map for criminals and terrorists to access these secure buildings. But let me also say that I am confident that the results of this undercover investigation being made available to the affected agencies and the public is the fastest way to improve security.

I know there are those that question our doing this now, but I must tell you that having heard the responses I have heard in the last 24 or 48 hours to this, it is indeed in my judgment—and I think most of those with whom I have spoken—imperative that the word get out. The culture, the customs of those who are in law enforcement, who happen to work in the security area, of letting somebody come through easily who they think is a fellow law enforcement officer simply is unacceptable.

Page 10 PREV PAGE TOP OF DOC

The message has to be sent out there much more rapidly and to many more people than simply the agencies in question here today because what we found, again, is a system-wide failure—not just the 19 of 19 or the two airports—but the probability, since it has been so uniform, that virtually any Federal, State, or local building that is secure or supposed to be secure or any airport can and would be penetrated by these same methods by those who know how to do it.

So the word needs to get out and the agencies need to be on the ball and make the correction and train those officers that are on the job. Otherwise, all of us are going to feel awful on a day when something like this happens for real with the bad guys in charge instead of us.

With that in mind, I am looking forward to hearing from our witnesses.

I yield to Mr. Scott, our ranking member, for his opening statement.

[The prepared statement of Mr. McCollum follows:]

PREPARED STATEMENT OF BILL MCCOLLUM, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF FLORIDA, AND CHAIRMAN, SUBCOMMITTEE ON CRIME

Good afternoon. This hearing of the Subcommittee on Crime will come to order.

Page 11 PREV PAGE TOP OF DOC

Today's hearing provides a timely opportunity for Congress to examine just how secure our secure agencies and buildings really are. We'll also have a chance to look into how easily available bogus police badges are, and how they can be put to dangerous use to penetrate secure federal agencies.

For some time, I've been concerned with the fact that stolen and counterfeit police badges are readily available on the Internet and from other commercial sources, and that they can be used by criminals, terrorists, and foreign intelligence agents for illegal purposes, including penetrating our nation's most secure government buildings, airports and other facilities. Legislation addressing this concern is currently pending before this Subcommittee. With this concern in mind, seven weeks ago I requested that the General Accounting Office investigate the potential security risk to secure Federal facilities posed by the use of such badges.

During the investigation that ensued, undercover OSI Special Agents targeted 19 secure Federal buildings and two major airports posing as plain- clothed law enforcement officers. In every case, these agents were able to enter agency buildings while claiming to be armed and carrying briefcases, which were never searched and were big enough to be packed with large quantities of explosives, chemical or biological agents. The agencies penetrated included the CIA, the Pentagon, the FBI, the Justice Department, the State Department, and the Department of Energy. The agents were simply waived around the metal detectors. In many cases, they had the run of the buildings once they were inside, including the offices of department secretaries. The agents drove a rental van into the courtyard of the Main Justice without the van being inspected or searched. The van was parked in the courtyard, and the agents left it while they went inside the building. On a single day, they succeeded in penetrating eight secure buildings. The havoc that could have been wreaked by actual terrorists doing the same is chilling to consider.

Page 12 PREV PAGE TOP OF DOC

For the two airports whose security was compromised, agents obtained boarding passes and firearm permits to carry weapons onboard the flights for which they had purchased tickets. Like the Federal buildings they entered, they carried briefcases that were never x-rayed. They walked right up to the door that led down the gangway to the airplane. Nothing stood between them and the aircraft. They had fooled everyone.

The agents' method was simple. They entered these buildings by flashing fake law enforcement badges and credentials and passing themselves off as Federal agents or local police officers. They assembled their bogus credentials by buying badges on the Internet and other sources and by using off-the-shelf computer graphics programs to generate official looking I.D. cards. They then placed the badges and credentials in small leather cases and went to work. To the untrained eye, these fake badges and credentials look like the real thing. They are not perfect counterfeits by any means. They were not intended to be perfect copies of the real thing. That fact is very disturbing. What these agents did a lot of people could do too. Certainly members of a foreign intelligence service or a terrorist organization could do it.

I must say, I find the easy availability of these badges to be disconcerting. In fact, if you were to get on line right now and go to E-bay's web site, you would find more than 600 police badges available for sale. There are dozens of other

web sites where badges can be purchased.

Earlier this week, I held a closed-door briefing for the agencies whose security had been compromised in order to make known the details of how their building and airport security had been penetrated. At that briefing, preliminary recommendations were presented on how to immediately close these gaping security holes, and I am pleased to report that steps have already been taken to begin to address the problem. As we will hear from our witnesses in just a moment, many of the recommendations are neither complicated nor expensive. They're really just common sense.

Page 13 PREV PAGE TOP OF DOC

What concerns me most about this investigation is that the undercover investigators were 19 for 19 with the agencies they targeted and two for two with the airports targeted. These findings point to a system-wide breakdown that is unaaceptable. This week, we are having major counter-terrorism exercises in Washington, D.C. involving a wide range of sophisticated simulated terrorist attacks. That is all well and good, but these efforts to detect and prevent terrorist attacks cannot overlook the obvious. Our secure buildings must have minimal security safeguards in place. Roaming around the halls of secure buildings, unescorted, and into Cabinet Members offices with unchecked briefcases doesn't cut it. The bottom line is that we have learned that far too many of our secure facilities where top secret and sensitive information is kept have an open door policy. As of this week, that is beginning to change.

I do want to state at the outset that the testimony presented today will be limited in certain important respects, so as to avoid providing a road map for criminals and terrorists to access these secure government buildings. But let me also say, I am confident that the results of this undercover investigation being made available to the effected agencies and the public is the fastest, most effective way to improve security.

Mr. **SCOTT.** Thank you, Mr. Chairman.

Mr. Chairman, we have the same interest in protecting the public and our Government employees and buildings from terrorists and other threats. However, I have to express concern over whether or not a public hearing is a proper vehicle for addressing security problems at Government buildings, particularly when this hearing comes only 2 days after the agencies received the initial information regarding this problem.

Page 14 PREV PAGE TOP OF DOC

Mr. Chairman, I remain concerned that the proliferation of the information through this hearing may actually serve to undermine rather than enhance the security of these facilities. I would think that our first priority would be to ensure that these agencies, as well as others not targeted, have had a realistic chance to learn of and address security deficiencies of the type GAO will report today.

To be sure, let me make it clear that I support efforts to enhance security at our agencies through security audits of the type undertaken by the GAO. When I was approached about my interest in working with the subcommittee on this matter, I thought it was good, Crime Subcommittee oversight activity, which could be very helpful to the agencies in their efforts to protect their operations and the public. However, I am skeptical of the suggestion that a public hearing at this time would contribute to security.

In addition to having a "gotcha" tone to it, holding this hearing quickly after telling the agencies what was found may place them in a position of having security vulnerabilities exposed before they have had a reasonable opportunity to fix the problem, particularly when some of those problems may not have a quick fix.

I have no doubt that the GAO has structured its public report in a manner designed to avoid revealing information

which may put the facilities they have targeted in harm's way. But I am sure that some of the targeted agencies may reasonably feel that this approach exposes them to additional risk. I am as interested as anyone else in having the public business conducted in public, but there are some things—such as safety and security procedures—which require prudence.

Page 15 PREV PAGE TOP OF DOC

I am told by some security experts with whom I have consulted that much of the public facility security system rests upon those with ill motives not knowing the capabilities of the system. Unfortunately, it appears now that information in the report, which will be the basis for today's hearing, which was marked "restricted" has actually had wide distribution, including coverage in the media. Hopefully, this hearing will not invite problems which might not otherwise have occurred without this hearing.

In any event, Mr. Chairman, I pledge complete cooperation with you in helping our Federal agencies address the concerns raised at today's hearing.

Mr. **MCCOLLUM.** Thank you very much, Mr. Scott.

Mr. Hyde, do you have any opening remarks?

Mr. **HYDE.** I have none.

Mr. **MCCOLLUM.** Does any other member of the committee have any opening remarks?

Mr. Barr?

Mr. **BARR.** Thank you, Mr. Chairman.

There was something that came to my mind when I read the paper and we talked about this hearing today and it is a book called "Unlimited Access" which came out in its first edition several years ago by a former decorated FBI agent, Gary Aldrich, who had been in charge of security clearances and security matters at the White House at the end of the Bush administration and the beginning of the Clinton administration.

Page 16 PREV PAGE TOP OF DOC

The reason that this book came to mind, Mr. Chairman, was that several years ago Mr. Aldrich, who was very, very familiar with the need for property security clearances and the need for starting at the top and working down to develop and implement a culture of being security conscious, which began breaking down almost as soon as this administration took office.

For example, as Mr. Aldrich noted in his book, the function of approving and issuing security clearances and permanent passes was done in a loose and dangerous way. We are now reaping, 5 years later, the problems that Mr. Aldrich told us first about several years ago.

And while I commend you, Mr. Chairman, for the investigative work you have caused to happen to highlight some of the specific breaches of security that has given rise to this hearing today, and while that certainly is important, I fear, Mr. Chairman, that the problems we are seeing here are systemic problems. They are endemic problems. They are problems that we see at the Department of Energy, which is fearful of requiring foreign nationals to even wear security badges because they might object to it as being somehow insensitive.

And we see it with regard to the lack of proper security procedures that have given rise to the most troubling instances of espionage—the most damaging instances of espionage that our Nation has seen in the post-World War II era, and that is the communist Chinese espionage and theft of vital national security secrets involving the most sensitive nuclear technology as well as technology involving detection of nuclear submarines.

These are all related, Mr. Chairman, and until we, as a Nation, demand that the highest offices in this land implement proper security procedures and insist that the proper security procedures remain in place, and that they are in fact adhered to, we are going to continue to see problems like this.

Page 17 PREV PAGE TOP OF DOC

So while it is important to focus on the specific security breaches, that is really just the tip of the iceberg, Mr. Chairman. I fear for our Nation's security if we don't get a handle on this. Hopefully, today this will not be an end but instead a beginning to addressing the systemic problems with this administration that have resulted in tremendous damage to our Nation's security. I guess the best that can be said is that we have been very, very lucky that we have not had a major incident as a result of the complete breakdown of concern for security by this administration.

I thank you, Mr. Chairman, for bringing this to our attention and for beginning the process, hopefully, of undoing and repairing some of the tremendous damage to the fabric of our Nation's security that has been the hallmark of this administration.

Mr. **MCCOLLUM.** Thank you, Mr. Barr.

Ms. Jackson Lee.

Ms. **JACKSON LEE.** Thank you very much, Mr. Chairman.

I am here today to join in a bipartisan effort to do simply one thing: to save lives. I am as interested in the proprietary and intellectual aspects of security issues that are being misused, abused, or utilized for improper purposes, but I am here today to save lives. I want to thank the chairman for the insight of providing an opportunity for this information to be utilized in a positive manner to collaborate with agencies to ensure that we protect those who utilize the services and those who work for those agencies.

Page 18 PREV PAGE TOP OF DOC

Might I say that I am well aware that we live in a free country governed by the first amendment that allows us to freely associate and to travel. And we have to keep that in mind when we begin to talk about securing our Nation in order to protect ourselves. Americans have always been inclined to opt for freedom of access and freedom to travel.

So this is an important issue we are dealing with. I appreciate the concern of this chairman for the practice of selling stolen and counterfeit badges on the Internet and other sources and the potential use of these items for illegal purposes. I have been concerned about illegal actions on the Internet for a long time and have legislation accordingly.

But I am also concerned, as the ranking member has indicated, about what we do here today in light of these hearings. The reason why my fear has accelerated is that I woke up this morning with news station after news station airing the sensitive issues that have been brought to light. The ranking member noted that we might even tune into CNN.com for the actual data we are talking about today.

This makes it very difficult when my focus is to save lives. I realize the media has its responsibility to report the news. However, I know it is likewise our responsibility as elected officials to ensure that we direct our attentions to ensuring again the safety of all those within our borders.

The GAO has yet to develop a final recommendation on the proper cause of action. It doesn't mean that I don't appreciate the work they are doing. In fact, as I look forward to hearing them—and I will have to depart briefly for another pressing meeting that I am engaged in—I want to make sure that as we proceed we make no personnel or agency —some 21 who have been violated, if you will—scapegoats. I am told that the chairman was very persistent, along with the ranking member on this well.

Page 19 PREV PAGE TOP OF DOC

We are here to cure, we are here to fix, we are here to save lives. I believe that ranking member Scott's recommendation that we go to recommendations first by GAO in order to adhere to our ultimate concern of saving lives, providing safe and secure places, of keeping data away from those who could do harm to us might have been the direction to take. But I will add my commitment, in light of the tragedies we have faced—PanAm 103, Oklahoma City, American embassies—to the chairman and to this committee and to this Congress and to the American public that we will work diligently to ensure that although we believe in the first amendment, that we provide protection against the likes of something like this, which I would test and ask anyone to challenge and see whether or not they could detect.

Whether this is falsified or in fact an accurate bag, this is what we are facing and it is an important issue.

With that, I hope that this hearing will help us do one thing: make us safer and more free at the same time.

I yield back the balance of my time, Mr. Chairman. I would also ask that my statement in its entirety be submitted into the record and as well offer some immediate apologies for having to step away and will hopefully join this hearing as it is proceeding.

I thank you and I yield back.

Mr. **MCCOLLUM.** Without objection, your prepared statement will appear in the record.

Page 20 PREV PAGE TOP OF DOC

[The prepared statement of Ms. Jackson Lee follows:]

PREPARED STATEMENT OF SHEILA JACKSON LEE, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF TEXAS

Mr. Chairman, the recent light that has been shed on the Breaches of Security at Federal Agencies and Airports by the General Accounting Office's (GAO), Office of Special Investigation (OSI) is extremely disturbing to me.

The GAO's security test of federal agencies resulted in the OSI being able to breach security at each of the nineteen (19) federal agencies it visited, and two (2) airports.

Mr. Chairman, let me commend you on your insight in calling for an investigation into these security breaches. Your concern regarding the practicing of selling stolen and counterfeit police badges on the internet and other sources, and the potential to use these items for illegal purposes including breaching the security at through the vessels of our Nation's security is very alarming, to put it mildly, and has led us here today to hold an oversight hearing on these breaches.

I too, have been concerned over the use of the internet to conduct criminal activity as well as to profit from it, and have drafted legislation which touches on some of these concerns.

I hope that this subcommittee can join together as it has on many occasions to work to resolve these problems.

Page 21 PREV PAGE TOP OF DOC

Mr. Chairman, the GAO's success in breaching the security of every federal site visited is disturbing and needs to be immediately addressed by the agencies. However, I believe that a public hearing on this topic at this time will cause an even greater security risk, by publicly identify the manner and method in which a person could breach the security of a federal building.

Mr. Chairman, my apprehension and fear became a reality this morning when I turned on the television. to hear news station after new station airing these sensitive security related breaches to the public, and inherently to the criminals, terrorists, and foreign intelligence agents who would seek to wreak havoc within our nation's borders.

I am not denouncing the media, for they are merely doing their job. However, we as the elected members of the American people who took an oath to uphold the Constitution of the United States and to protect our countries borders and national security must do our jobs as well. The GAO has yet to develop final recommendations on the proper course of action agencies should take, and the agencies have not had time to revise their security procedures.

I must say that the publicizing of these security deficiencies is extremely puzzling.

Ranking Member Scott has made it good recommendation that we post-pone this hearing to give the GAO time to make its security recommendations and for the federal agencies and airports in question to implement these security recommendations.

Page 22 PREV PAGE TOP OF DOC

To do otherwise would be tantamount to handing the keys to the doors of this country's national security over to the likes of those who were involved in the bombings of the federal building in Oklahoma, Pan Am Flight 103 over Scotland, and the American Embassies in Africa.

Mr. Chairman, let us not rush through the elevator doors of this insightful investigation to find that the elevator is not there. Let us work together to ensure the safety and security of this great nation.

Thank you.

Mr. **MCCOLLUM.** Mr. Gekas, you are recognized.

Mr. **GEKAS.** Thank you, Mr. Chairman.

Contrary to the statements made by the gentleman from Virginia and the lady from Texas as to the questionability of holding these hearings so soon after the committee has had reason to hold this hearing, I believe that the level of awareness raised immediately, as we speak, by the chairman's action and by Chairman Hyde in joining into the function of this meeting is very salutary and will save lives. It may have already put into motion certain improvements that will save lives.

Judging from the same news reports upon which the gentleman from Virginia relies on his questioning this hearing, I

say that saving lives may already have been occurring as we prepared for this meeting. I think that a blow for awareness has been struck here today, that the entire American public is better off by reason of this episode, which will bear immediate increased security guarding that will be essential to all of us.

Page 23 PREV PAGE TOP OF DOC

I thank the Chair for holding the hearing.

Mr. **MCCOLLUM.** Thank you, Mr. Gekas.

Mr. Hutchinson?

Mr. **HUTCHINSON.** Thank you, Mr. Chairman.

As someone who worked in these agencies, someone who tried to go to the Department of Justice a few years ago and had a difficult time getting through the magnetometer, this is quite startling to see these revelations.

I think particularly, from America's standpoint, we are investing hundreds of millions of dollars to secure these buildings and the personnel who work in there, certainly after the tragedy at Oklahoma City—and I think that is appropriate. But I think what is important from today's hearing and this investigation is that we make that investment work.

I appreciate what the chairman has said, that we have to look at better training. I think it is important that we not understate the problem, nor overstate the solution that is demanded. In this case, it appears to me that it is not a failure of equipment, it is not a failure of investment, nor is it a lack of personnel being committed to security. It is really a matter of training and policy.

So I think today I will look forward to hearing these witnesses to look at what policy changes are needed.

Page 24 PREV PAGE TOP OF DOC

Again, I appreciate the way the chairman has conducted this and the ranking member in looking at it from the standpoint of what we can work on together to improve the policies that protect each of these dedicated public servants.

I yield back.

Mr. **MCCOLLUM.** Thank you very much, Mr. Hutchinson.

We are now ready for our first and only panel today. I am pleased to welcome Robert Hast, Assistant Comptroller General for Special Investigations with the U.S. General Accounting Office. As Comptroller General, he oversees the Office of Special Investigations and was in charge of the undercover operation that is the subject of today's hearing. Prior to joining the GAO, Mr. Hast was the vice president of security for Mastercard International. He is a 20-year veteran of the U.S. Secret Service where he served in numerous capacities, including supervising the Presidential Protection Division during the Reagan administration. He is a graduate of Columbia University, where he was captain of the football team.

Mr. Hast is accompanied by two special agents with the Office of Special Investigations at GAO. Patrick Sullivan is an assistant director of OSI and participated in the undercover operation. He was in the Secret Service for 23 years, retiring in 1999 as Deputy Special Agent in charge of the Counterfeit Division. He is a graduate of John Jay College of

Criminal Justice, University of New York.

Page 25 PREV PAGE TOP OF DOC

Ronald Malfi is also an assistant director of Office of Special Investigations and participated in the undercover operation. Like his two colleagues here today, he is a 22-year veteran of the Secret Service where he was the supervisor of the Intelligence Division. He is a graduate of Saint John's University and received his master's degree at John Jay College of Criminal Justice.

I want to welcome you all this afternoon.

Before we commence the testimony, I do need to swear you in because this is an investigative hearing.

[All witnesses respond in the affirmative.]

Mr. **MCCOLLUM.** Let the record reflect that all three answered in the affirmative to that oath.

At this point in time, Mr. Hast, I want to turn this over to you for any testimony you may see to give us. Your written testimony is admitted into the record in its entirety. Without objection, it is so ordered and entered. You may proceed to summarize or give your testimony today.

We again thank you very much for what you have done and being here today.

STATEMENT OF ROBERT HAST, ASSISTANT COMPTROLLER GENERAL, SPECIAL INVESTIGATIONS, OFFICE OF SPECIAL INVESTIGATIONS, UNITED STATES GENERAL ACCOUNTING OFFICE

Page 26 PREV PAGE TOP OF DOC

Mr. **HAST.** Thank you, Mr. Chairman and members of the subcommittee.

I am pleased to be here today with my associates, Ron Malfi and Pat Sullivan, to discuss our findings with respect to the subcommittee's request that we investigate the potential security risk to the United States posed by the use of stolen or counterfeit law enforcement badges and credentials. Specifically, you expressed concerns that such badges and credentials are readily available for purchase on the Internet and from other public sources and could be used by criminals, terrorists, and foreign intelligence agents to gain access to secure Government buildings and airports.

To address these concerns, you asked us to acquire fictitious law enforcement badges currently available to the public and to create fictitious identification to accompany the badges. You also asked that our special agents, in an undercover capacity, attempt to gain access to secure facilities in such a manner that they could have introduced weapons, explosives, chemical/biological agents, listening devices, or other hazardous material.

We conducted our work March through May of 2000. Our undercover agents were 100 percent successful in penetrating 19 Federal sites and 2 commercial airports. We were able to enter 18 of the 21 sites on the first attempt. The remaining three required a second visit before we were able to penetrate the sites.

At no time during the undercover visits were our agents' bogus credentials or badges challenged by anyone. At each visit, our agents carried bogus badges and identification, declared themselves as armed law enforcement officers, and gained entry by avoiding screening. At least one agent always carried a valise.

Page 27 PREV PAGE TOP OF DOC

Sixteen of the sites we visited contained the offices of cabinet secretaries or agency heads. At 15 of these sites, our undercover agents were able to stand immediately outside the suites of the cabinet secretary or agency head. In the five instances in which our agents attempted entry into such suites, they were successful. At 15 of the sites, our agents entered a rest room in the vicinity of these offices and could have left a valise containing explosives or other such materials without being detected. Except for one agency, we made no attempt to determine whether any of the cabinet secretaries or agency heads were present at the time we visited the agencies.

In all but three sites, escorts were not required and our agents wandered throughout the buildings without being stopped. At the three sites that required escorts, our undercover agents were permitted to keep their declared firearms and carry their unscreened valises. Indeed, at all three of the sites, our agents were able to enter a rest room carrying the valise without the escort. At one of the sites, our agents later separated from their escort and walked through the building for about 15 minutes without being challenged.

At a Federal courthouse, our agents were waved through a magnetometer but not screened. A briefcase that one of the agents carried was not checked. The agents were escorted to a gun box room which they were permitted to enter alone. They were then instructed to lock their weapons, but no one supervised or observed the actual surrender of the agents' weapons.

At the two airports we visited, our agents had tickets issued in their undercover names on commercial flights. These agents declared themselves as armed law enforcement officers, displayed their spurious badges and identification, and were issued law enforcement boarding passes by the airline.

Page 28 PREV PAGE TOP OF DOC

Our agents then presented themselves at the security checkpoint and were waved around the magnetometer. Neither the agents nor their valises were screened.

Our undercover teams consisted of two or three agents. In all cases, upon entering the Federal facility, our undercover agents declared themselves as law enforcement officers, stated the name of their purported agency, stated that they were armed, and in most cases displayed both the bogus badge and a bogus credential. In all but two of the agencies we penetrated, the suite number of the cabinet head or agency head was listed in public documents.

Our agents drove a rented mini-van into the courtyard entrance of a Department and only one agent showed identification. They and the vehicle were permitted entry without being screened. They parked the van in the courtyard and proceeded to the Department head's office. They entered the office and asked the receptionist whether the head of the Department was in and told the receptionist that they were friends of the Department head with whom they had previously worked. They were told that the Department head was not in. The agents then requested and received a tour of the agency head's suite and conference room.

Three agents drove a sedan to a site and only the driver showed identification. They were issued a VIP parking pass and parked a few yards from the building entrance. The vehicle was not checked. The agents then walked into the building, avoided the magnetometer, and verbally declared themselves as law enforcement officers. Only one agent showed identification. All three were issued "no escort required" visitor passes. Two agents carried valises, which were also not checked.

Page 29 PREV PAGE TOP OF DOC

They then proceeded to the hallway outside the Secretary's office. Two agents briefly entered the Secretary's suite

before excusing themselves. All three agents were able to enter the Secretary's conference room and other offices without being challenged.

Our agents, one of whom carried a valise, entered a historic site posing as a police detective and was waved past the magnetometer. After a few minutes, the agents were approached by a uniformed police officer. He said that because they were local police officers, not Federal agents, they would have to check their firearms in a lock box in the basement. Our agents stated that they did not have time to stay and left the building.

At the two airports we visited, our agents had tickets issued in their undercover names on commercial flights. These agents declared themselves as armed police detective sergeants, displayed their spurious badges and identification, and were issued law enforcement boarding passes by the airline representative at the ticket counter. The procedure after checking in at the ticket counter varied at each airport.

At one airport, our agents walked unescorted to the airport's security checkpoint, showed their badges to a contract security guard, and were waved around the magnetometer. A contract guard supervisor was then called to examine the undercover agents' credentials and law enforcement boarding passes. The agents then logged themselves in a book kept behind the security checkpoint. Neither the agents nor their valises were screened and they walked unescorted to their departure gate. At no time were they required to present themselves to an airport police officer.

At the second airport, our undercover agents were required to show identification to an airline contract security guard. The airline contract security guard then escorted our undercover agents from the ticket counter to the security checkpoint and called for a local police officer. The contract security guard waited with our agents for about 10 minutes until the police officer arrived.

Page 30 PREV PAGE TOP OF DOC

The police officer then examined our agents' credentials and escorted them around the magnetometer. Neither the agents nor their valises were screened. They then proceeded unescorted to their departure gate.

Mr. Chairman, this concludes my prepared statement. We would be happy to answer any questions that you or members of the subcommittee may have.

[The prepared statement of Mr. Hast follows:]

PREPARED STATEMENT OF ROBERT HAST, ASSISTANT COMPTROLLER GENERAL, SPECIAL INVESTIGATIONS, OFFICE OF SPECIAL INVESTIGATIONS, UNITED STATES GENERAL ACCOUNTING OFFICE

Mr. Chairman and Members of the Subcommittee:

I am pleased to be here today to discuss our findings with respect to the Subcommittee's request that we investigate the potential security risk to the United States posed by the use of stolen or counterfeit law enforcement badges and credentials. Specifically, you expressed concerns that such badges and credentials are readily available for purchase on the Internet and from other public sources and could be used by criminals, terrorists, and foreign intelligence agents to gain access to secure government buildings and airports.

To address these concerns, you asked us to acquire fictitious law enforcement badges currently available to the public and to create fictitious identification to accompany the badges. You also asked that our special agents, in an undercover capacity, attempt to gain access to secure facilities in such a manner that they could have introduced weapons, explosives, chemical/biological agents, listening devices, or other hazardous material.

Page 31 PREV PAGE TOP OF DOC

Scope and Methodology

In conducting our investigation, we collected background information from public sources on various federal government sites in the Washington, D.C., area and other geographical areas. We established a list of potential target locations based upon the sites' involvement in national security, intelligence, and criminal justice and their symbolic or historic significance. We also included major commercial airports. All sites require screening of visitors. All sites appeared to have magnetometers and x-ray machines at the security checkpoints for screening visitors and valises, e.g., briefcases and baggage.

We visited some of these sites as private citizens, i.e., members of the "general public," to observe the screening procedures and conduct surveillance from public areas. We set out to determine if some sites employed additional security measures, such as outer-perimeter checkpoints, roving patrols, or countersurveillance teams.

We also developed information about each site based on public source information, the Internet, and pretext telephone calls.

We acquired the counterfeit and/or unauthorized law enforcement badges that you asked us to obtain from public sources. We created multiple counterfeit sets of credentials representing local and federal law enforcement agencies.

In April and May 2000, we performed our undercover work at 19 federal facilities and 2 major commercial airports.

Page 32 PREV PAGE TOP OF DOC

Results in Brief

Our undercover agents were 100 percent successful in penetrating 19 federal sites and 2 commercial airports. We were able to enter 18 of the 21 sites on the first attempt. The remaining 3 required a second visit before we were able to penetrate the sites.

At no time during the undercover visits were our agents' bogus credentials or badges challenged by anyone. At the 21 sites that our undercover agents successfully penetrated, they could have carried in weapons, listening devices, explosives, chemical/biological agents, devices, and/or other such items/materials.

At each visit, our agents carried bogus badges and identification, declared themselves as armed law enforcement officers, and gained entry by avoiding screening. At least one agent always carried a valise.

Sixteen of the sites we visited contained the offices of cabinet secretaries or agency heads. At 15 of these sites, our undercover agents were able to stand immediately outside the suites of the cabinet secretary or agency head. In the 5 instances in which our agents attempted entry into such suites, they were successful. At 15 of the sites, our agents entered a rest room in the vicinity of these offices and could have left a valise containing weapons, explosives, and/or other such items/materials without being detected. Except for one agency, we made no attempt to determine whether any of the cabinet secretaries or agency heads were present at the time we visited their agencies.

Page 33 PREV PAGE TOP OF DOC

At a federal courthouse, our agents were waved through a magnetometer but not screened. A briefcase that one of the

agents carried was not checked. The agents were escorted to a gun box room, which they were permitted to enter alone. They were then instructed to lock their weapons, but no one supervised or observed the actual surrender of the agents' weapons.

At the two airports we visited, our agents used tickets that had been issued in their undercover names for commercial flights. These agents declared themselves as armed law enforcement officers, displayed their spurious badges and identification, and were issued "law enforcement" boarding passes by the airline representative at the ticket counter. Our agents then presented themselves at the security checkpoints and were waved around the magnetometers. Neither the agents nor their valises were screened.

Background

We acquired badges from public sources to use in this case. The badges included a movie prop of a police department badge, which is in similitude to genuine badges. In addition, we acquired a counterfeit federal badge not in similitude to a genuine federal badge and a drug task force badge that is in similitude to a genuine badge.

We created counterfeit law enforcement identification using commercially available software packages or information downloaded from the Internet. We used a standard computer graphics program, an ink-jet color printer, and photographs. After we printed the identifications, we laminated them. The credentials we created bear no likeness to any genuine law enforcement credentials.

Page 34 PREV PAGE TOP OF DOC

Sites Penetrated

We penetrated 21 sites—19 federal departments/agencies and 2 commercial airports. (See app. I.) We were successful at each site and our agents' bogus credentials and badges were not challenged by security. (See app. II.) The sites were selected on the basis of their involvement in national security, intelligence, and criminal justice, and in their symbolic or historic significance. All sites require screening of visitors. All sites appeared to have magnetometers and x-ray machines at the security checkpoints for screening visitors and valises, e.g., briefcases and baggage.

How Penetration Was Accomplished

At all but two agencies, our undercover team consisted of two agents. Three agents worked undercover at the other two agencies. In all cases, upon entering the federal facilities, our undercover agents

"declared" themselves as law enforcement officers,

stated the name of their purported agency,

stated that they were armed, and

in most cases, displayed both a bogus badge and a bogus credential.

In some cases, only one agent had to show a badge, and the other agent was waved in by a security guard. At least one agent always carried a valise. In all cases, our agents were able to enter the facility by being waved around or through a magnetometer, without their person or valise being screened.

Page 35 PREV PAGE TOP OF DOC

We were able to enter 18 of the 21 sites on the first attempt. The remaining 3 required a second visit before we were able to penetrate the sites.

In all but three sites, escorts were not required and our agents wandered through the buildings without being stopped. At the three sites that required escorts, our undercover agents were permitted to "keep" their declared firearms and carry their unscreened valises. Indeed, at all three of the sites, our agents were able to enter a rest room carrying a valise without the escort. At one of the sites, our agents later separated from their escort and walked through the building for about 15 minutes without being challenged.

At 15 of the 16 locations that contained the offices of cabinet secretaries or agency heads, our agents were able to stand immediately outside the suite of the cabinet secretary or agency head. At the 5 locations at which our agents attempted entry into such suites, they were successful. At 15 sites, our agents entered a rest room in the vicinity of these offices and could have left a valise containing weapons, explosives, and/or other such items/materials without being detected.

In all but two of the agencies we penetrated, the suite numbers of the cabinet head or agency head were listed in public documents.

Examples of Sites Penetrated

Our agents drove a rented minivan into the courtyard entrance of a department and only one agent showed identification. They and the vehicle were permitted entry without being screened. They parked the van in the courtyard and proceeded to the department head's office. They entered the office and asked a receptionist whether the head of the department was in and told the receptionist that they were friends of the department head, with whom they had previously worked. They were told that the department head was not in. The agents then requested and received a tour of the agency head's suite and conference room.

Page 36 PREV PAGE TOP OF DOC

Three agents drove a sedan to a site and only the driver showed identification. They were issued a VIP parking pass and parked a few yards from the building entrance. The vehicle was not screened. The agents then walked into the building, avoided the magnetometer, and verbally declared themselves as law enforcement officers. Only one agent showed identification. All three were issued "No Escort Required" visitor passes. Two agents carried valises, which were also not checked. They then proceeded to the hallway outside the Secretary's office. Two agents briefly entered the Secretary's suite, before excusing themselves. All three agents were able to enter the Secretary's conference room and other offices without being challenged.

Our agents, one of whom carried a valise, entered a historic site posing as police detective sergeants and were waved past the magnetometer. After a few minutes, they were approached by a uniformed police officer. He said that because they were local police officers, not federal, they would have to check their firearms in a lock box in the basement. Our agents stated that they did not have the time to stay and left the building.

At the two airports we visited, our agents had tickets issued in their undercover names on commercial flights. These agents declared themselves as armed police detective sergeants, displayed their spurious badges and identification, and were issued "law enforcement" boarding passes by the airline representative at the ticket counter. The procedure after checking in at the ticket counter varied at each airport.

At one airport, our agents walked unescorted to the airport's security checkpoint, showed their badges to a contract security guard, and were waved around the magnetometer. A contract guard supervisor was then called to examine the undercover agents' credentials and law enforcement boarding passes. The agents then "logged" themselves in a book

kept behind the security checkpoint. Neither the agents nor their valises were screened and they walked unescorted to their departure gate. At no time were they required to present themselves to an airport police officer.

Page 37 PREV PAGE TOP OF DOC

At the second airport, our undercover agents were required to show identification to an airline contract security guard. The airline contract security guard then escorted our undercover agents from the ticket counter to the security checkpoint and called for a local police officer. The contract security guard waited with our agents for about 10 minutes until the police officer arrived.

The police officer then examined our agents' credentials and escorted them around the magnetometer. Neither the agents nor their valises were screened. They then proceeded unescorted to their departure gate.

Mr. Chairman, this concludes my prepared statement. We would be happy to answer any questions that you or Members of the Subcommittee may have.

Mr. **MCCOLLUM.** Thank you very much, Mr. Hast, for your testimony today.

I assume you speak on behalf of Mr. Sullivan and Mr. Malfi and that we are ready for questions?

Mr. **HAST.** Yes.

Mr. **MCCOLLUM.** I recognize myself for 5 minutes of questions, then.

Page 38 PREV PAGE TOP OF DOC

First of all, I want to commend you for this. This was an extraordinary thing that you were called upon to do and you did it very professionally. I think all of us in the Nation owe you a debt of gratitude for carrying out what some call a sting operation—really probably not technically that, but essentially giving us information that would not have otherwise been available to us.

There are a lot of questions any of us could ask you. I want to ask a couple of them, though, that I think are particularly pertinent.

You have described some very lax procedures, and you obviously penetrated every single agency you went to. All three of you were Secret Service agents at one time, in fact, for a number of years. I am curious to know if you believe that you could have used these same badges to bluff your way into the White House. If not, why not?

Mr. **HAST.** I do not believe that we would have been able to get into the White House. One of the reasons we didn't try is because, as you said, we are all former Secret Service agents and know the personnel there very well. I do not believe that the White House would have been penetrated by this kind of scam. For security reasons, I would not want to get into details as to why this would not work at the White House.

Mr. **MCCOLLUM.** But needless to say, there are methods being used over there that are different than those methods which you encountered. And that is the point. There are ways of stopping this from happening and I wanted to point that out.

Had the briefcases you carried had explosives in them, Mr. Malfi and Mr. Sullivan, how much damage do you think could have been done to the buildings you entered?

Page 39 PREV PAGE TOP OF DOC

Mr. **MALFI.** I think they would have done a lot of damage if they were placed in certain locations. We had access to most of these buildings and had the ability to place things where we wanted to.

Mr. **MCCOLLUM.** Were you in these buildings long enough to plant listening devices, if you had wanted to do that?

Mr. **MALFI.** That is correct.

Mr. **MCCOLLUM.** And did you get close enough to a Department head or agency head to assassinate them?

Mr. **MALFI.** We didn't ascertain if agency heads were there at the time that we made the penetrations. We had access to certain parts of their outer offices or their suites. If we had planted devices there, I would assume that if we wanted to check that with a scheduling, damage would have occurred in that area also.

Mr. **MCCOLLUM.** I am curious about something else, too. Maybe I should ask this of Mr. Hast.

You were able to enter rest rooms near cabinet secretaries' or agency heads' offices I think in 15 of the sites that you gave us. Do you have any suggestions you can offer to improve the vulnerability in that sort of situation? Suppose someone did penetrate one of these agency buildings and got all the way to that point. What could be done? What kind of security? Do you have an opinion about that?

Page 40 PREV PAGE TOP OF DOC

Mr. **HAST.** While it is difficult to make recommendations after having done this so recently—and we would like to look at it very closely—there are some things that are done in various buildings, such as cipher locks on the rest rooms, thereby only employees that knew the combination to the cipher lock would be able to enter, or you would have to go to a secretary or someone that would be able to take a visitor and let them in the rest room.

Mr. **MCCOLLUM.** It is my understanding that you actually did penetrate eight of these agencies in a single day. Is that correct?

Mr. **HAST.** That is correct, sir.

Mr. **MCCOLLUM.** Can any of you tell us which agencies you did in that single day?

Mr. **SULLIVAN.** This if from memory, Mr. Chairman, but I believe it was FEMA, HHS, Energy, DOT, FAA, National Archives, and Labor. But that is from memory, sir.

Mr. **MCCOLLUM.** But can you imagine the kind of damage that could have been done to our national security had all those agencies been penetrated by a foreign operative in a single day intent upon disrupting this Nation's commerce and disrupting our communications systems and our law enforcement in those areas that you just described? Couldn't that have been devastating if in every one of those you had put a time bomb or planted something in at the same time?

Page 41 PREV PAGE TOP OF DOC

Mr. **SULLIVAN.** Mr. Chairman, in some of those agencies, we got to the rest room near the agency or cabinet member's suite and we could have planted a device to have them all go off at 5:00 p.m. or 4:00 p.m. Yes, sir, you are

correct. We could have had all the devices go off at the same time.

Mr. **MCCOLLUM.** Before my time is up—and I am about to yield to Mr. Scott—you have a tape, I believe, that demonstrates a little of what you did. Mr. Sullivan, I believe you have that tape. Can you show that for us, please?

Mr. **SULLIVAN.** Sure.

[Video presentation.]

Mr. **SULLIVAN.** This is our penetration of the INS headquarters. We walk in, identify ourselves as police detectives, we are waved around the magnetometer, and we proceed back to the appointment desk.

The next site is HHS. I approach the security desk, Agent Malfi goes right to the elevators, I flash a credential, and Agent Malfi is holding something up in his hand—that is actually a badge.

The next site is FEMA. We identified ourselves as Federal agents at this location. The magnetometer is behind the security desk, they check us in and we avoid the magnetometer.

Page 42 PREV PAGE TOP OF DOC

NASA is next. We identify ourselves as police officers to a security guard in the lobby and he enables us to walk right around the magnetometer and we proceeded right to the administrator's suite.

DOT. This is the employee's entrance at the Department of Transportation. Agent Malfi is already on the elevator. This uniformed guard is telling me that if I am armed I have to get a special law enforcement pass and he tells me to tell my partner that. He is already on the elevator and already up on the ninth floor.

Department of Energy. We are at the Government employee visitor desk. We identified ourselves as Federal agents and were waived around the visitor's desk. We encountered a uniformed police officer who then gave us unescorted badges and we proceeded up to the Secretary's suite.

FAA. We are waved past the magnetometer and were given an employee's pass to roam the building.

National Airport. We are approaching the ticket counter. We identify ourselves as police detectives. In the next scene, we are coming up to the security checkpoint. I am in the lead and identify ourselves as police officers and we are waved around the magnetometer. Both of us are carrying bags, as you can see.

Next is Orlando International Airport. We are at the ticket counter. We required a law enforcement boarding pass from the airline employee at the ticket counter. At the magnetometer checkpoint our credentials are just checked by a police officer and you can see us walking around the magnetometer. Both Agent Malfi and I are carrying large bags.

Page 43 PREV PAGE TOP OF DOC

Department of State. We are at the appointment desk posing as police detectives awaiting to get issued our credentials.

Lastly—this is from last week's *Police Week*—a stand that was selling police badges.

That concludes the tape, Mr. Chairman.

[Video presentation complete.]

Mr. **MCCOLLUM.** I thank you for showing this.

Before I turn this over to Mr. Scott for questions, I do have one clarifying question that you reminded me of by that.

I can't and don't want to get into the airport security methodology in detail, but am I correct—because I think you have told us this in the private briefing—that there was a distinct difference between the procedures at the Orlando International Airport and at Reagan National. In other words, there was a greater laxity at Reagan National, in general? Is that correct?

Mr. **SULLIVAN.** That is correct, Mr. Chairman. There were inconsistent procedures. For example, at National a police officer did not have to examine our credentials and at Orlando a police officer had to examine them.

Page 44 PREV PAGE TOP OF DOC

Mr. **MCCOLLUM.** Again, I don't want to get further into that. You still penetrated both places, but one followed procedures more in line than the other did.

With that in mind, Mr. Scott, I yield to you.

Mr. **SCOTT.** Thank you, Mr. Chairman.

Mr. Chairman, our public servants have a very difficult challenge. They are trying to conduct the public's business as courteously as they possible can. Obviously, some agencies, by their very nature, require a higher level of security than others.

The witnesses have testified that the White House would have a different security procedure. But with other agencies, some have national security secret military implications and others would not. You would expect the security systems to possibly reflect those differences.

They have reported problems. I will be interested in the response from the agencies, particularly those responses that require legislative action and funding that we can address directly as legislators. But I understand the various agencies are reviewing their procedures and hopefully before this hearing have already made changes.

I yield back.

Mr. **MCCOLLUM.** Thank you very much, Mr. Scott.

Page 45 PREV PAGE TOP OF DOC

Mr. Hyde?

Mr. **HYDE.** Thank you, Mr. Chairman.

I want to thank you for your thoughtfulness in holding this hearing. I understand the problem mentioned by Mr. Scott that there is some question as to the advisability of going public. But on the other hand, at bottom, this problem involves an attitude—a national attitude—that puts security the lowest issue on the totem pole. And the only way to wake people up is to shock them. This is shocking. But the attitude of complacency toward security has to end because this country can fall without a shot being fired if some of our most secret places can be penetrated, as they obviously can be.

The problem with our adversaries is that they haven't learned to hire people who look like policemen. You fellows don't fit the profile. That is to your advantage.

Security is inconvenient. You have to wait in line while they x-ray your bag and look at your wallet, and see that you are not carrying weapons. But we are going to have to get used to paying that price, and the public is going to have to get used to it. These hearings are a step toward changing the attitude we have of complacency.

It is pretty scary, not just what you did, but the whole security atmosphere in this town. When the former director of the CIA, Mr. Deutsch, can put top secret material on his computer and then take it home. When the CIA let this fellow, Aldrich Ames, live pretty high on the hog for years, nobody was suspicious. They never heard of a net worth audit, I guess.

Page 46 PREV PAGE TOP OF DOC

But we are going to have to upgrade security. It is going to have to be a very serious, high-level concern of every agency, particularly the sensitive ones. We are going to have to recruit people who can make a career, as you people have—we need thousands of people who have the training, the desire, the energy, and the street smarts to protect our security. We need to upgrade the salary levels, recruit people, and train them.

So this tension between freedom and making America a big hotel lobby cannot really continue in a world where we are despised by certain people and certain countries where they have the capacity—increasingly so—to wreak devastating harm on us. You don't need an intercontinental missile, you just need a vial of anthrax and a diplomatic pouch to knock a city out. We have to start thinking about that.

You, gentleman, have performed a signal service in bringing this to our attention. I think if there is some shock value to this, thank God.

I thank you gentlemen.

Mr. **MCCOLLUM.** Thank you, Mr. Hyde.

Mr. Chabot?

Mr. **CHABOT.** I will defer to Mr. Barr at this time and ask that you come back to me.

Page 47 PREV PAGE TOP OF DOC

Mr. **MCCOLLUM.** Mr. Barr is recognized for 5 minutes.

Mr. **BARR.** Thank you.

This is the identification that we were each given as a Member of Congress. It also serves as our voting card. When I go to the airport, the ticket agents spend an eternity, sometimes, looking at these things. They look at it every which way to Sunday. I don't know if that is just because they like me so much or because they have never seen one, or what not. But they are very, very diligent about looking at identifications before you board an aircraft, asking the questions about the bags having been in your possession and if you have received anything from a stranger.

From what you are telling us today, our country's security might be better off if we hire ticket agents from airlines to serve as security officers at our Federal buildings. And I don't say that with any humor. We seem to be doing a much better job of protecting the security of our aircraft in terms of who gets on them and ensuring that their identification has

been verified than allowing people of utterly unknown identification gain access to not only the most sensitive of our Government agencies but the most sensitive areas within those sensitive buildings.

What you all have told us today is very, very frightening. As Mr. Hyde said, and as I said in my opening, what Mr. Aldrich—and I don't know if you all know Mr. Aldrich, but he was a very, very distinguished special agent with the FBI, very highly decorated. He wrote the book "Unlimited Access" several years ago, detailing how starting at the very top levels of our Government—and you can't get any higher than the President of the United States in the White House—a very lackadaisical attitude toward the granting of security clearances, allowing people without security clearances, without badges, to roam the halls of the White House and other executive buildings.

Page 48 PREV PAGE TOP OF DOC

What we seem to be doing now is that 7 years later from the time that Mr. Aldrich first chronicled this it has worked its way down to the level of access to virtually every Federal agency. Security under this administration's watch is not only a low priority, it seems to be a non-priority.

It is my experience—I spent several years with the Department of Justice as a United States Attorney and back in the 1970s several years with the CIA—back in those days, when we had administrations, whether Democrat or Republican—I have served under both and was honored to do so—security was something that was hammered at constantly for employees. We had to have regular and periodic security clearance renewals. We had to receive periodic briefings. Supervisors were responsible for ensuring that the burn bags were prepared every evening, that the computers were turned off, that employees had their badges, and so forth.

And, while even back in those days, I remember that there were security breaches out at the CIA headquarters in Langley and these were also noted in the media, the fact of the matter is that we had a culture back in those days where security was something that was important to our Government. It was something that was hammered away at constantly with our employees. It was not something to be ashamed of or to be sensitive or to feel you were being singled out for insensitivity if you were required to wear a badge. It was to be expected.

And I think also—and would ask all of you if you agree with the fact—proper security, a successful security program, is something that has to be consciously discussed. It has to be refreshed in the minds of the employees. And if you don't have a proper regard for security at the top, it is very difficult for proper security to be practiced all the way down the line.

Page 49 PREV PAGE TOP OF DOC

Is that accurate in terms of security, whether it is in a private setting or a Government setting?

Mr. **HAST.** I believe that is accurate. I would only like to add that I don't think the operation we conducted is an indictment of the overall security of all of these facilities. I think the request by this committee was a very good one because these badges provide a unique method of entrance that I don't think has been looked at. But I don't think the fact that someone using law enforcement credentials in being able to beat the security is an indictment of the overall security.

Many of these people followed procedures, they have just never looked at the possibility. And I think as technology moves forward and it is easier to make copies—I mean, the whole face of counterfeit money has changed because of the ease in which things can be reproduced. It has gone to identification. It is now easy to make this type of identification. We are going to have to look at this and to move up.

But I think what we found is a unique hole in the security that can be fixed. But we certainly haven't looked at it close

enough, and I don't we would indict the entire security systems in these buildings. I think for the most part they are very good.

Mr. **BARR.** With regard to the specific credentials that you all developed here—and we have a number of them up here—was there an effort made to ensure that these credentials did mirror, to the greatest extent possible, the actual authenticate credentials?

Page 50 PREV PAGE TOP OF DOC

Mr. **HAST.** No, we did not. We made bogus credentials and did not make any attempt to make them exactly like the real credentials.

Mr. **BARR.** Could I ask the chairman's indulgence to ask one final question?

If in fact you all had been private citizens—not Government employees specifically authorized to conduct this operation and therefore you didn't violate any laws in what you were doing—had you been private citizens, not so immunized, would there be a number of laws that you would have violated had you conducted these operations as private citizens if you were seeking to harm a Government person or building?

Mr. **HAST.** Impersonating a Federal officer is a Federal crime. Impersonating a State officer is not.

Mr. **SULLIVAN.** It is not a Federal crime, but we did have a counterfeit Federal badge, which would be currently a Federal crime. But the counterfeits of the State badges are not currently a Federal crime.

Mr. **BARR.** Is it a Federal crime to obtain unauthorized access to a secure Federal facility under current law?

Mr. **SULLIVAN.** I don't believe so.

Page 51 PREV PAGE TOP OF DOC

Mr. **MALFI.** I think the most that we could have been charged with is trespassing.

Mr. **BARR.** Thank you, gentlemen.

Thank you, Mr. Chairman.

Mr. **MCCOLLUM.** Thank you very much, Mr. Barr.

Mr. Gekas?

Mr. **GEKAS.** Thank you, Mr. Chairman.

In the capitol itself, here, the electronic devices are practically at every entrance, insofar as I have been able to determine. Yet a Member of Congress can walk in and deference is granted to that Member by allowing him to move outside of the purview of that, and the guard recognizes the Member and doesn't feel it is necessary. After all, this is the home—the house—of the Members.

Do you believe, in the discoveries that you made, that the recognition factor for law enforcement officers is a big weakness in all of this?

Mr. **HAST.** Yes. I think the fact that people are allowed entrance carrying weapons when there are law enforcement

credentials issued in every State, county, and local jurisdiction. There are too many law enforcement credentials for someone to recognize all of them. It would be impossible.

Page 52 PREV PAGE TOP OF DOC

So if you are going to allow law enforcement officers in the building armed, you have a problem. Unlike the capitol police here being able to recognize the Members, there is no way to recognize all the law enforcement officers in the United States.

Mr. **GEKAS.** Is it predictable that the recommendations that the agencies are right now, even at this moment, preparing for beefing up their security measures—is it predictable that they will be taking some measures on not even permitting fellow law enforcement officers to avoid the screening? Do you think they will be doing some of that? Or do you hope that they do? Or will you counter-recommend if they don't through our committee?

Mr. **HAST.** I think they will all look at their security. I know the FBI issued a press release yesterday saying that law enforcement officers will no longer be able to carry weapons into the FBI. There will be lock boxes outside the magnetometers. I wouldn't be surprised to see other agencies do the same thing.

Mr. **GEKAS.** So already your work and the exposure that this committee has been giving to this problem has borne some results, almost an immediate check-up, shall we say, on posing law enforcement officers.

At the White House—you had mentioned this—I remember going there and my ego was hurt when they did not recognize me and they made me go through the electronic device. Then I learned that even if they had recognized me, they would have put me through that. That is probably a model. I am glad that happened. It is a model that ought to be followed in the capitol itself.

Page 53 PREV PAGE TOP OF DOC

I have no further questions. I thank the Chair.

Mr. **MCCOLLUM.** Thank you very much, Mr. Gekas.

I just want to follow up with a couple of very quick ones.

Mr. Hast, one of Mr. Gekas' questions was close to this one, but I want to clarify it.

You guys look like cops. You walk the walk. You do. You bear yourselves that way. How hard would it be for John Q. Public to get into one of these buildings carrying a badge and credentials like you did?

Mr. **HAST.** I think it would be difficult for the average person to carry himself, but I think a trained, intelligence officer, a terrorist—someone who had training would be able to do that.

But I do want to mention that while you say that we look like law enforcement officers, Ron Malfi spent most of his career posing as a criminal buying counterfeit money. [Laughter.]

Mr. **MCCOLLUM.** So he looks more like a criminal.

I still think you look pretty much like a cop to me. You could go on a television show and play the role, Mr. Malfi. You would have fooled me, anyway.

Page 54 PREV PAGE TOP OF DOC

But the bottom line is that you think that perhaps a foreign intelligence agent or a terrorist could bluff his way in, but you don't suspect that the average John Q. Public would have nearly the success you had, would you?

Mr. **HAST.** No, I don't. I think you would have to have some training.

Mr. **MCCOLLUM.** I have one other question here.

Mr. Malfi, during your penetrations of the various Federal facilities and airports, were you or any of your other undercover team members ever challenged?

Mr. **MALFI.** No, we were not.

And one of the things I would like to make clear is that when we talk about the fact that we were posing as law enforcement agents and allowed access to certain locations, this was not a police courtesy that was done with a wink and nod or something that was not supposed to be done but they allowed because of some sort of brotherhood. The reality is that police officials have to carry guns, just like doctors have to carry syringes and medication. So they have to allow entry into certain locations because this is a tool of the trade.

Unfortunately, the amount of badges that are out there makes it thoroughly impossible for someone to be able to recognize all of them and to be able to tell counterfeits from the genuine thing. We discovered a hole in the system. Hopefully that hole will be addressed. And as Bob Hast said earlier, with some tweaking, this type of penetration should be able to be avoided in the future.

Page 55 PREV PAGE TOP OF DOC

Mr. **MCCOLLUM.** You and Mr. Hast and Mr. Sullivan have truly provided a public service, as I said earlier.

I have in front of me—and this is just one illustration—this was pulled off the web today—a whole series of places you can buy badges. There are color pictures of them and we didn't reproduce them in color, but they are there. I don't know that I ought to advertise the particular web site. There is a whole page of badges that are priced at various levels—$15, $16—here is a concealed weapons permit and identification set, Connecticut State Police, for $30. New, it says. New Massachusetts State Police psychologist—you get one for $16. New Connecticut State Police, $29.

How come Connecticut costs more than Massachusetts? I don't know. [Laughter.]

Mr. **MCCOLLUM.** But here is a Florida lieutenant for only $15. I don't know about that.

But the bottom line is that they are here, they are available, they are readily reproduced, and it is something we are going to have to address on our end of it. But no matter how strong an action this committee takes with regard to whether we outlaw some of this or not, the security questions, the training question, the importance of that is really, really what this hearing is about. What you and we have done today is alert the American public and, most importantly, those agencies other than these 19 and these 2 airports that they have a problem if they don't get their security officers into a room and into some proper training. And while they might not be able to identify every single badge, surely they can perform procedures that are far better than they are performing today. And surely they challenge somebody once in a while.

Page 56 PREV PAGE TOP OF DOC

Well, I want to thank all the panel for being here today. This has been a very important hearing for us.

With that in mind, this hearing is adjourned.

[Whereupon, at 3:11 p.m., the subcommittee was adjourned.]

SPEAKER INDEX CONTENTS INSERTS

CONTENTS SPEAKERS INSERTS

INSERTS SPEAKERS CONTENTS

NO INSERTS IN THIS HEARING