STATE DEPARTMENT DOMESTIC SECURITY LAPSES AND STATUS OF OVERSEAS SECURITY ENHANCEMENTS

HEARINGS

BEFORE THE

COMMITTEE ON INTERNATIONAL RELATIONS HOUSE OF REPRESENTATIVES

ONE HUNDRED SIXTH CONGRESS

SECOND SESSION

MAY 11 AND MAY 17, 2000

Serial No. 106–162

Printed for the use of the Committee on International Relations

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

U.S. GOVERNMENT PRINTING OFFICE
67–827 CC WASHINGTON : 2000

COMMITTEE ON INTERNATIONAL RELATIONS

BENJAMIN A. GILMAN, New York, *Chairman*

WILLIAM F. GOODLING, Pennsylvania
JAMES A. LEACH, Iowa
HENRY J. HYDE, Illinois
DOUG BEREUTER, Nebraska
CHRISTOPHER H. SMITH, New Jersey
DAN BURTON, Indiana
ELTON GALLEGLY, California
ILEANA ROS-LEHTINEN, Florida
CASS BALLENGER, North Carolina
DANA ROHRABACHER, California
DONALD A. MANZULLO, Illinois
EDWARD R. ROYCE, California
PETER T. KING, New York
STEVE CHABOT, Ohio
MARSHALL "MARK" SANFORD, South Carolina
MATT SALMON, Arizona
AMO HOUGHTON, New York
TOM CAMPBELL, California
JOHN M. MCHUGH, New York
KEVIN BRADY, Texas
RICHARD BURR, North Carolina
PAUL E. GILLMOR, Ohio
GEORGE RADANOVICH, California
JOHN COOKSEY, Louisiana
THOMAS G. TANCREDO, Colorado

SAM GEJDENSON, Connecticut
TOM LANTOS, California
HOWARD L. BERMAN, California
GARY L. ACKERMAN, New York
ENI F.H. FALEOMAVAEGA, American Samoa
MATTHEW G. MARTINEZ, California
DONALD M. PAYNE, New Jersey
ROBERT MENENDEZ, New Jersey
SHERROD BROWN, Ohio
CYNTHIA A. MCKINNEY, Georgia
ALCEE L. HASTINGS, Florida
PAT DANNER, Missouri
EARL F. HILLIARD, Alabama
BRAD SHERMAN, California
ROBERT WEXLER, Florida
STEVEN R. ROTHMAN, New Jersey
JIM DAVIS, Florida
EARL POMEROY, North Dakota
WILLIAM D. DELAHUNT, Massachusetts
GREGORY W. MEEKS, New York
BARBARA LEE, California
JOSEPH CROWLEY, New York
JOSEPH M. HOEFFEL, Pennsylvania

RICHARD J. GARON, *Chief of Staff*
KATHLEEN BERTELSEN MOAZED, *Democratic Chief of Staff*
KRISTEN GILLEY, *Professional Staff Member*
JILL N. QUINN, *Staff Associate*
MARILYN C. OWEN, *Staff Associate*

CONTENTS

WITNESSES

THURSDAY, MAY 11, 2000

WEDNESDAY, MAY 17, 2000

APPENDIX

THURSDAY, MAY 11, 2000

Prepared statements:

WEDNESDAY, MAY 17, 2000

Prepared statements:

CURRENT CHALLENGES TO STATE DEPARTMENT SECURITY—PART I

THURSDAY, MAY 11, 2000

HOUSE OF REPRESENTATIVES,
COMMITTEE ON INTERNATIONAL RELATIONS,
Washington, DC.

The Committee met, pursuant to notice, at 10 a.m. In Room 2172, Rayburn House Office Building, Hon. Benjamin A. Gilman (Chairman of the Committee) presiding.

Chairman GILMAN. The meeting will come to order. Good morning.

I regret that we are about to embark on a series of votes on the floor. It may take as much as an hour, and it will delay our hearing, and they are 5-minute votes based on amendments that were adopted last night. I will open the hearing, and then we will have to recess until the votes are concluded. I regret the delay for our witnesses.

Today our Committee examines current challenges to State Department security. The nature of these challenges is not a mystery. Over the last 2 years, there have been numerous well-known serious security failures at the State Department.

In 1998, a person in a brown tweed coat grabbed highly classified documents from an office in the Secretary of State's suite. That man and the documents have not been found.

Last year, a Russian spy was discovered outside the Main State building listening to a bugging device planted in a seventh floor conference room. Of course, last month saw the revelation of a missing laptop computer that contained highly classified information. That laptop has not been found.

Again, in 1999, we were told that a computer software program written by citizens of the former Soviet Union was purchased by the State Department on a sole-source contract and installed in posts throughout the world without the proper security and vetting procedures. That program had to be removed from each and every post. To this day, we have not received an explanation of just why and how that happened.

The news media has extensively uncovered each of these events. What is less known, however, is that the officials in the State department have known for years that security at the State Department was vulnerable to just these kinds of incidents.

In a March 1998, State "town hall meeting," Under Secretary for Political Affairs Thomas Pickering, called a department-wide wake-up call about security issues. Another top official noted that pro-

moting individual responsibility is going to require more security training and rigorous followup; and, of course, that is very true.

Later that year, a report by the Inspector General highlighted problems in the State Department's Bureau of Intelligence and Research [INR] and made recommendations to fix them. Today, INR has not yet responded to that report.

Another report by the Inspector General in 1999 recommended broader changes to the State's security policy, including the transfer of authority over "codeword" level material from INR to the Diplomatic Security Bureau; and although this report was issued in September 1999, its recommendations were at first rejected by the Department. They were not adopted until April 2000, well after the celebrated laptop had been found to be missing.

On November 17, 1998, a new State policy requiring escorts for all visitors was announced. It requires "all visitors with the exception of active U.S. Government agency personnel who display proper photo identification shall be escorted at all times." Six days later, that policy was rescinded. Nine months later, it was reimplemented.

Just last week the Secretary of State held another Department-wide Town Hall Meeting on security matters; and while her tone and words were appropriately tough, we cannot help but wonder if they will have any more impact than those of Mr. Pickering and other top officials at the 1998 Town Hall Meeting.

A few days before the most recent town meeting, the Secretary issued a document that revealed, on close analysis, that it had decided not to measure its security performance on the basis of the number of security compromises detected. In addition, the Department failed to make progress on reducing a scandalous backlog of security investigations. It is now moving toward, in effect, a 15-year cycle for security updates, rather than 5-year government standard.

The Department did, however, manage to significantly exceed the target it set for itself of reducing its inventory of overseas vehicles over 5 years old. So we are left to ask: Are the Department's priorities appropriate? Should we be surprised that a casual attitude toward security is part of the Department's culture if its budget priorities practically shout that information security is not the Department's major concern?

We have learned that despite recent changes in security policy, reporters from foreign news media have access to many parts of the State building without any supervision. Indeed, we are informed that press personnel with identification cards have a 24-hour access to the building, including weekends and holidays.

In other words, the new escort policy has a big hole, a big gap. You can lead an elephant through it. It is no secret that foreign intelligence agencies do use reporters as agents. During the Cold War, the KGB agents routinely used reporters' credentials as cover for many of their activities. The recent book entitled The Sword and the Shield by Christopher Andrew and Vasili Mitrokhin details numerous incidents of Soviet spies who have posed as reporters. It is a safe bet that the KGB's successor agencies in Russia today use the very same techniques.

No security policy at State will be adequate until foreign journalists are appropriately escorted, just like other visitors beyond the normal press areas in the State Department.

A secure State Department, however, is not just a matter of changing a few policies. It is the daily culture of our diplomats that are going to have to change. Every person in the State Department from maintenance personnel to Ambassadors to the Secretary of State must reprioritize and make security their top concern.

This does not mean that policymakers in top jobs are off the hook. Far from it. Leadership must come from the top, and the responsibility for the current, disastrous conditions of State Department security lies with the Secretary's office and with her top aides.

I want to quote from an anonymous letter received by this Committee just this week from a Foreign Service employee: "For the poor security environment at the U.S. Department of State to improve only one thing is required, that being for State to seriously and publicly punish several senior officials, including at least two current Ambassadors, for security violations. The punishments would have to be real and hurt, to include firings and criminal prosecutions."

I trust that Department of State—and we have several of its top officials here today—will give us advice and will consider these thoughts that we just expressed. Our Nation must not tolerate any further security violations at the State Department or at any agencies. Department officers need to realize that both the lives of innocent people and national security put at risk when they are haphazard in following elementary procedures.

The consequences for compromising national security secrets, whether intentional or inadvertent, are great. They result in costly investigations, damage relations with other Nations and, most gravely, possible mortal danger for Americans serving our Nation abroad.

In closing, I would like to quote a former Ambassador to the United States from France, Jules Cambon, who said, "The day secrecy is abolished, negotiation of any kind will be impossible."

It is no exaggeration to say that the very mission of this State Department, to carry out our Nation's foreign policy, has been placed in a perilous atmosphere at the present time.

Is there any other Member—Mr. Smith.

Mr. SMITH. Thank you very much, Mr. Chairman. I want to thank you for convening this very important hearing of the full Committee on this very, very troubling issue.

Let me just say I want to welcome our very distinguished panel. I see Ambassador Stapleton Roy, who many of us visited when he was in China, then in Indonesia, a very accomplished diplomat. We are very happy to have you here.

Secretary Carpenter—I would just note for the record, Mr. Chairman, Secretary Carpenter appeared before our Subcommittee, the International Operations and Human Rights Subcommittee, back on March 12 of last year and gave compelling testimony, along with Admiral Crowe, with regard to the growing threat to our embassies and assets abroad. He pointed out at the time—and I would like to quote him—because I think it is very timely and is a problem

that still exists and has actually worsened—the terrorist threat is global, lethal, multidimensional and growing.

Our analysts estimate that during the last 12 months, there were 2,400 threats against U.S. interests overseas. As you pointed out, Mr. Secretary, that was a 100 percent increase. And for the record, I think it is important to give credit where credit is due.

I used your compelling testimony of that day, over the course of the next several weeks and months, in support of H.R. 3427, the State Department Reauthorization Bill. This bill had a significant plus-up for overseas embassy security, as a matter of fact, we provide in Section 1 and Section 6 $5.945 billion over 5 years. I have to tell you, and I want to say this in gratitude, your testimony was very effective and woke up a large number of people who perhaps had not realized just how bad things had gotten and how much in need we were of providing that important money. So I want to thank you for that.

As you know, the President signed that legislation in November, and it is law. It does authorize the money and I think in a bipartisan way we will continue to make that money available to do this.

And of course, Mr. Chairman, the issue at hand is the laptop computer, the Inspector General's report, and you have covered most of the bases as was pointed out in the findings. The INR has not effectively discharged its responsibilities for the protection of sensitive compartmented information and is not well structured or staffed to oversee the management of the ESI security.

I was particularly concerned, and you made note of it as well, that on the issue of escorts inside the State's building, that the Under Secretary of State for Management, Tom Pickering, rescinded on November 23 a policy that was published about a week before, on November 17 of 1998. That is very, very troubling, and hopefully we can get to the bottom of that. It seems to me, if we have people unescorted walking around the building that raises very severe questions about who might have access to very sensitive information.

I think, Mr. Chairman, you have outlined the issue. During questions and testimony we will certainly delve into it further. But I did want to publicly thank Secretary Carpenter for that testimony and the good work that he and the others do. It did lead, as a consequence, to that legislation, so I want to thank him.

I yield back the balance of my time.

Chairman GILMAN. Thank you, Congressman Smith.

Mr. Lantos.

Mr. LANTOS. Thank you, Mr. Chairman.

I want to commend you for holding this hearing, and I want to bring to my colleague's attention a development that unfolded just a few hours ago which makes security at the State Department and throughout our government of extreme importance.

A few hours ago, in Moscow, agents of the KGB have raided the headquarters of the one free media outlet in Russia. This should not be surprising in view of the fact that the new Russian President Putin spent 15 years in the KGB and has surrounded himself with KGB operatives and is singularly incapable of accepting criticism of either Russian policies in Chechnya or anywhere else.

I look forward to the testimony of our distinguished witnesses and, having had a long-standing professional relationship with the Secretary, I can only say that I know from my own personal knowledge that no Secretary of State has been more intent on maintaining maximum security with respect to all sensitive materials than our current Secretary Madeline Albright.

It is always the head of the operation who is responsible for anything that goes wrong, and Secretary Albright has accepted that responsibility. But as we begin this hearing I think it is important for us to realize that, given her background and her attitudes and her experience, her own personal commitment to maintaining the highest professional standards of security within the Department is unquestioned; and I know that this hearing will unfold in the context of that knowledge.

I thank you, Mr. Chairman.

Chairman GILMAN. Thank you, Mr. Lantos.

Since we have a series of votes, the Committee will now stand in recess until the votes are concluded. Thank you very much for your patience and indulgence.

[Recess.]

Chairman GILMAN. Committee will come to order.

I want to apologize for the number of votes that were on the floor, which necessitated the recess that we have just gone through.

We are pleased to have with us today a distinguished panel and allow me to introduce them.

Before I introduce the panelists, our Ranking Minority Member, the gentleman from Connecticut, Mr. Gejdenson, has an opening statement. Mr. Gejdenson.

Mr. GEJDENSON. Thank you, Mr. Chairman. Thank you for calling this hearing.

Obviously, it is always a difficult challenge in a democratic society to balance our needs for security and also have a society open enough that we can operate in a democratic manner. But all of us are alarmed by the disturbing lapses in security in the last several years at the State Department, potentially compromising national security—listening devices, individuals in unauthorized areas, a laptop disappearance, workers given maybe too free access to areas important to national security.

We need not simply to figure out there but elsewhere in the government, in the post-Soviet era, to recognize there is still an important need for security, and we have to make sure that we have the resources and the structure in place to make sure that our national secrets are protected and at the same time that we move forward and make our systems of government accessible to the citizens, to the press and to those who are authorized to have access.

I certainly hope that everybody took the Secretary of State's statement and her several comments in the town meeting with the State Department officials to heart, that we all have to participate in this process. She said that, unlike academia, a 99 percent success rate just isn't acceptable here. It is a difficult challenge, but I think we all recognize that we have to be successful 100 percent of the time.

I thank the Chairman for calling the hearing and look forward to hearing the witnesses.

Chairman GILMAN. Thank you, Mr. Gejdenson.

Now we will proceed with our panelists.

I am pleased that we have with us the Honorable Jacquelyn Bridgers, Inspector General in the Department of State. Ms. Bridgers was sworn in as the Inspector General in 1995. She has been before this Committee many times, and we appreciate the valuable work of your good offices.

We will also hear from Assistant Secretary for the Bureau of Intelligence and Research, Stapleton Roy. Ambassador Roy has a distinguished 44-year history in the Foreign Service, having served as Ambassador to Singapore, to China and to Indonesia before taking over as Assistant Secretary for the Intelligence and Research Bureau.

We also welcome Assistant Secretary for Diplomatic Security David Carpenter. Mr. Carpenter assumed his position as Assistant Secretary in August 1998 following a 26-year career in the U.S. Secret Service. He is the first person to hold that position and has a professional background in the protection and security fields.

Finally, we welcome as our fourth witness Timothy Bereznay, a Section Chief in the National Security Division of the Federal Bureau of Investigation. Mr. Bereznay has been with the Bureau for 24 years. In his current assignment he has management oversight responsibilities for investigations related to counterintelligence and espionage allegations that pertain to our Department of State.

We appreciate the willingness of our panelists to appear before our Committee on this very important topic.

I will ask Ms. Williams-Bridgers to proceed with a summary of your statement, and following the statements we will proceed to questions. Any of the panelists who want to summarize, we will make your full statement a part of the record. Ms. Bridgers.

STATEMENT OF THE HONORABLE JACQUELYN L. WILLIAMS-BRIDGERS, INSPECTOR GENERAL, U.S. DEPARTMENT OF STATE

Ms. WILLIAMS-BRIDGERS. It is indeed a pleasure to be before the Committee again. Mr. Gejdenson, Mr. Chairman, thank you very much for the opportunity to testify before the Committee on the Department of State's security programs as they relate to the protection of sensitive intelligence in national security information.

The Department has implemented a diligent effort to enhance the physical security of our overseas missions. Today U.S. missions are significantly more secure than they were 20 months ago. Based on our overseas inspections we have found that our embassies generally do a good job of protecting classified information.

Recent lapses at Main State clearly demonstrate that attention must now be given to address vulnerabilities in protecting sensitive intelligence and national security information on the domestic front.

The Secretary's recent decision to transfer authority for protection of intelligence-related material from the Bureau of Intelligence and Research to the Bureau of Diplomatic Security implements an important corrective action that we recommended to ensure proper safeguards for our most sensitive intelligence-related information.

Mr. Chairman, in your invitation to this hearing you asked me to discuss my office's assessment of the security environment within INR and the Department overall, the division of security responsibilities between INR and DS, the Department's security incident disciplinary process, the effectiveness of the disciplinary process in deterring poor security practices, and the Department's responsiveness to OIG's recommendations.

In brief, OIG has found significant deficiencies in the handling of classified information that have perpetuated a lax security environment in the Main State headquarters building. Specifically, we found that ineffective access controls in the Main State headquarters building left offices vulnerable to the loss or theft of sensitive intelligence information and equipment by unescorted, uncleared visitors and contractors. A lack of adequate physical and procedural security measures in offices resulted in classified documents not being properly controlled and accounted for. INR was not fulfilling its security function and unit security officers in other bureaus were not enforcing security requirements, leading us to recommend a delegation of responsibility to DS for protecting highly classified information. Last, OIG found that disciplinary actions for security violations did not serve as a deterrent for lapses in security practices.

Let me focus first on the key security deficiencies we identified. Our review of the handling of classified information found that uncleared maintenance and repair and cleaning contractors are not always escorted when in offices where classified information is handled, processed and stored. This occurred even though there has long been a Department policy that escorts are mandatory in controlled access areas. Very few contractor personnel have clearances. We found that the vast majority of offices did not perform the escort function. In cases where escorting was performed, the degree of vigilance was inconsistent.

We also found that INR had not complied with required routine inspections of 140 Department offices where sensitive compartmented information was maintained or discussed. Also, none of the offices had received technical surveillance countermeasure inspections to determine whether listening devices had been implanted.

Our review also found that while SCI documents were distributed to 46 offices each morning, controls or procedures were not in place to ensure that all material was returned to an SCI facility and properly secured at the close of business. In addition, INR was not obtaining signed receipts to establish accountability for the documents and did not verify that all the documents were actually returned.

INR had also not complied with the Director of Central Intelligence directive regarding personnel security standards. Specifically, we found that INR had not complied with the requirements that only individuals with a need to know had access to SCI materials and that the results of background investigations be considered in making that determination.

We found that unit security officer [USO] responsibilities were not being performed because many USOs were not fully informed of their security responsibilities, and they did not believe that they had the authority to enforce security procedures. In 21 of 23 offices

inspected, there was no assurance that after-hours checks were performed or that classified documents were properly stored. Of 23 USOs we interviewed, 17 did not perform office security reviews. Only 5 of 23 offices escorted their uncleared cleaning staff. Only 11 of 23 regularly briefed their employees on security.

INR has not effectively discharged its responsibility for the protection of SCI. In our view, INR is not well structured or staffed to oversee the management of SCI's security.

The primary function of DS, however, is to ensure that people and information are properly protected. DS is already responsible for overseeing Department procedures for protecting classified information up to the Top Secret level. Further, DS has a cadre of trained security professionals. Therefore, the OIG recommended that the duty of safeguarding SCI should be delegated to DS.

Mr. Chairman, my office will be conducting a followup review later this year to determine the adequacy of the Department's response to all of our recommendations.

The Department's security incident program also has not been effective because security awareness and disciplinary actions have not been sufficient. Repeat offenders receive letters of warning and, depending on the gravity of the situation, they can continue to retain their security clearances allowing access to the most sensitive information in the Department.

We recommended that the Department strengthen security training and the disciplinary actions associated with security incidents.

In summary, I am encouraged by the actions taken by the Department recently to correct the physical and procedural security deficiencies at Main State that we have noted in our work. It is unfortunate, however, that lapses in security that were identified by OIG last year were not addressed in a more timely fashion. This delay no doubt may have contributed to an environment in which the most recent highly publicized breeches occurred. At this juncture, however, it is essential that the Department exercise vigilance and commitment to maintain and enforce the highest level of security awareness and compliance.

This concludes my short statement, and I would be glad to answer questions at the appropriate time.

[The prepared statement of Ms. Williams-Bridgers appears in the appendix.]

Chairman GILMAN. Thank you, Inspector General Bridgers.

Assistant Secretary Roy, Bureau of Intelligence and Research, please proceed.

STATEMENT OF AMBASSADOR J. STAPLETON ROY, ASSISTANT SECRETARY OF STATE FOR INTELLIGENCE AND RESEARCH, U.S. DEPARTMENT OF STATE

Mr. ROY. I am glad to have the opportunity to appear before you today with my colleague, Assistant Secretary Carpenter. We will be happy to discuss with you the Department's response to the disappearance of an INR laptop computer and other important security matters.

Let me begin by briefly reviewing the basic facts regarding the disappearance of the laptop computer. On January 31 of this year, a laptop computer containing highly classified information was dis-

covered to be missing from a secure area controlled by the Bureau of Intelligence and Research at the Department of State, or INR, which I head. This matter is under active criminal investigation by the FBI and the Department's Bureau of Diplomatic Security, or DS. I have asked all personnel of INR to cooperate fully with the investigation. That is our sole role. We not privy to the investigation's focus, its time line, or its findings, so I cannot speak to those issues.

In my testimony today, I will focus on four subjects which the Committee asked me to address in its invitation letter: First, the disappearance of the laptop. The laptop had been purchased in 1996 for the exclusive use of officers from other bureaus engaged in counterproliferation work who did not have access to classified workstations within INR. It was used and stored in an INR secure area because it contained highly classified information bearing on the proliferation of weapons and technologies of mass destruction and their associated delivery systems. Because of the sensitive information on it, the computer was not permitted to leave the INR secure area where open storage was authorized under applicable regulations.

On January 31, INR staff could not locate the laptop in response to a request by a would-be user from outside the Bureau. When a careful search of the office suite failed to locate the laptop, the office in question took immediate steps to interview all personnel in the office as well as officers from outside the Bureau who had been authorized to use the laptop.

Some of those approximately 40 officers were out of country on official business. They were queried by phone or cable. When these efforts failed to locate the laptop, INR's security branch chief launched a formal investigation and requested the office director to respond to a detailed list of questions. He also interviewed key individuals and developed a summary of relevant circumstances. When this internal investigative phase failed to locate the laptop, the INR security branch chief reported the circumstances to me, along with his recommendation that because of the potential compromise of classified information the matter be turned over to DS. I immediately approved this recommendation, and on February 10 INR requested DS to commence an investigation and notified the CIA Center for Security that a computer presumed to contain sensitive classified material could not be located.

All matters pertaining to the investigation are under the purview of DS and the FBI, and I am not privy to the details. We do not yet know how the laptop disappeared, whether it was removed by an employee authorized to work in the office, whether it was stolen for its material value or whether it was taken for the information on its hard drive.

Regardless of the circumstances, the loss of the laptop is inexcusable. It should not have happened. As the Assistant Secretary for Intelligence and Research, I am also the senior officer of the Intelligence Community in INR and in the Department of State. All personnel in INR from top to bottom have been indoctrinated and trained to be aware of their responsibility to safeguard the Nation's most sensitive secrets. Whatever the results of the investigation, it

is clear that we failed to exercise our responsibility to safeguard the computer and the classified information on it.

I particularly regret that Members of Congress first learned of the incident from the pages of the Washington Post. This was never our intention. That it happened is most unfortunate and is being looked into as part of our effort to draw lessons from this unfortunate experience.

Second, the Secretary's decisions in response to the loss. As a result of the circumstances I have just outlined, the Secretary took a number of steps affecting the Bureau that I head:

First, after consulting the Director of Central Intelligence, George Tenet, the Secretary decided that DS should take over from INR the responsibility for protection of sensitive compartmented information. I support this decision and am confident that DS will do the job well. We are working hand in glove with DS and the CIA to effect this transfer. In addition to improving security, I believe this will strengthen INR's ability to concentrate on what we do best, which is analysis and intelligence policy coordination.

In my view, this transfer of the SCI security function can be handled in a manner that will not conflict in any way with INR's responsibilities as a statutory member of the Intelligence Community. Indeed, since before the discovery that the laptop was missing, we had been working closely with DS to identify and formalize areas for enhanced cooperation.

Aside from the transfer of the SCI security function to DS, the Secretary also asked that in the investigation of the disappearance of the laptop, questions of accountability be examined carefully and appropriate recommendations be made for decision. Meanwhile, to enhance confidence in the review process, two INR office directors have been temporarily transferred to other duties. This is not a finding of fault. It is to ensure that as the investigation is conducted and remedial steps are taken there is full confidence in the process.

In addition, the Secretary directed that a number of other steps be taken to tighten security in the Department, which we can address at other points in our testimony here.

The security environment within INR. The Secretary held a town meeting at the Department on May 4 to stress once again that all Department employees must attach the highest priority to their security responsibilities. I had already reinforced this message in a meeting with the entire INR staff on April 26, and I am confident that everyone in the Bureau is conscious of the need to maintain a high level of security awareness at all times and that security is an inextricable and indispensable part of their jobs.

Mr. Chairman, you inquired in your invitation letter to me about the day-to-day procedures of monitoring classified information within INR. In accordance with the relevant directives, SCI security or control officers responsible for Sensitive Compartmented Information Facilities maintain records, manual or electronic, of external receipt and dispatch sufficient to investigate loss or compromise of SCI documents during transmittal.

Given the volume of classified and SCI material received daily in INR, we and DS have recognized the need to strengthen procedures for assuring document accountability. Earlier this year, we sought

and gained approval to hire additional document control specialists. Upon their entry on duty, they will work to ensure that both the theory and practice of document accountability within INR are fully in accord with Intelligence Community standards and requirements.

Following recess of the OIG report last September, the DCI's Community Management Staff offered to make available to INR a professional document control specialist to evaluate our existing staffing and document control procedures and to make appropriate recommendations. I understand the individual selected to assist us, expected to arrive in INR very soon, will come from the Defense Intelligence Agency, whose operational milieu is in important respects similar to that at State.

In regard to the management of and security procedures for construction or renovation projects at Main State, in INR this relates primarily to Sensitive Compartmented Information Facilities, or SCIFs. Here DCID 1/21 on Physical Security Standards for Sensitive Compartmented Information Facilities is the governing directive. The DCID requires that whenever a project is contemplated, a construction plan balancing threats and vulnerabilities must be reviewed and approved by the cognizant security authority. In my view, these requirements are time tested and appropriate provided they are, as they should be, rigorously observed.

The fourth subject you asked me to address was the INR Assistant Secretary's role as senior official of the Intelligence Community.

First, let me affirm that I see no statutory, regulatory or procedural barriers that need interfere with the ability of the Bureau of Diplomatic Security to carry out security responsibilities within INR. There are some fine points now being addressed, but they have not been implemented in any way within INR to the Bureau of Diplomatic Security. Nor should this impede INR's ability to perform its function as a member of the Intelligence Community.

As Members of this Committee may be aware, the Department of State is not a member of the Intelligence Community. Rather, it is INR within the Department that is a statutory member. As Assistant Secretary of INR, I am the senior adviser to the Secretary of State on all intelligence matters and responsive to her direction. At the same time, I have certain responsibilities to the Director of Central Intelligence that derive from my status as the Senior Official of the Intelligence Community within INR.

The authorities and responsibilities vested in SOICs, or Senior Officials of the Intelligence Community, are detailed in DCID 1/19—Security Policy for Sensitive Compartmented Information and Security Policy Manual. This directive states that intelligence organizations, as defined in Executive Order 12333, have the authority and are responsible for all aspects of security program management with respect to the protection of intelligence sources and methods and for implementation of the DCIDs for activities under their purview.

Hence, INR had previously maintained its own security program for intelligence sources and methods, while DS had developed and implemented security procedures on a broad range of security responsibilities that fall within its purview. Pursuant to the Sec-

retary's decision to transfer SCI security protection to DS, we are working with DS and CIA to develop the necessary procedures within the framework of the DCID.

In conclusion, let me stress once again that the Department of State is undertaking a top-to-bottom review of security procedures. INR is a part of that process and, working closely with DS, we are moving simultaneously on many fronts to ensure better security throughout the Bureau. As the Secretary said, a 99 percent grade on security is not a passing grade. Thank you.

[The prepared statement of Mr. Roy appears in the appendix.]

Chairman GILMAN. Thank you, Secretary Roy.

We are now pleased to hear testimony by the Honorable David Carpenter, Assistant Secretary for the Bureau of Diplomatic Security at the Department of State.

You may summarize your statement, put the full statement in the record, whatever you deem appropriate. Please proceed.

STATEMENT OF THE HONORABLE DAVID G. CARPENTER, ASSISTANT SECRETARY OF STATE FOR DIPLOMATIC SECURITY AND SENIOR ADVISOR TO THE SECRETARY OF STATE ON SECURITY ISSUES, U.S. DEPARTMENT OF STATE

Mr. CARPENTER. Mr. Chairman and Members of the Committee, I am appearing before you today to answer questions about the recent laptop incident. I am also prepared to discuss other domestic security issues affecting the Department of State.

I accepted the position of Assistant Secretary at the State Department with the full realization that the job would be challenging, but I could never have envisioned the enormity of that challenge. I doubt that there are many outside the agency who appreciate the magnitude of the task thrust upon DS, the complexity of the issues faced in managing a global security program responsible for the protection of so many lives, and the challenges in facing off against sophisticated espionage services as well as transnational organizations focused on the destruction of American interests around the world.

On a positive note, I was extraordinarily gratified by the capabilities and professionalism of the people working in the Bureau of Diplomatic Security. They are clearly first rate. But I was shocked to learn just how much the State Department's budget had been cut and, to my regret, how hard those budget and personnel cuts had hit DS. I found that DS had people in all areas of its responsibilities who, in my experience, were second to none in other similar agencies, but it became painfully obvious that DS, although challenged and dedicated, had far too few people to meet the challenges it was about to encounter.

Following the fall of the Soviet Union, DS was authorized to hire only a handful of agents, engineers and civil service security personnel. Twenty percent of DS positions worldwide were reduced. The worldwide guard program was decreased by 5 percent. Rules and regulations concerning security were loosened to the point that holding employees accountable for serious security issues became more difficult.

It is my assessment that the budget and personnel cuts had significantly eroded the Bureau's ability to fulfill even its most basic

services. They had reached the point that when there were major conferences in the United States requiring significant manpower to staff protective details, numerous operational offices had to be shut down to support this effort. In some respects, this type of scenario continues to this day.

Let me give you a few examples of how DS' programs were streamlined during that period. Among the activities affected was our office of counter intelligence. The number of positions was reduced from 41 to 26 and funding for the program was cut from $225,000 to $65,000. Staffing for programs in the Department that handle procedural and informational security issues was reduced by more than 50 percent. Our technical countermeasures programs suffered a similar fate as limited funding forced the Bureau to fund only priority life safety programs rather than to invest in upgrading its antiquated countermeasures program. The Department's reaction to imposed fiscal constraints and a popular opinion that the Cold War had ended and now the world was a better place had devastating consequences for DS programs.

In 1997, the Bureau's hiring picked up considerably and while it appeared that they were making strides in restaffing to the point of making it ready to meet its existing challenges, the bombings in East Africa occurred. Let me say that those bombings have dramatically changed the magnitude and intensity of our overseas security programs and the support of this Committee in regard to our specific needs has been much appreciated. As you are aware, nearly all of our new positions acquired since the bombings have been directed at overseas staffing or in support of our overseas operations, chiefly with antiterrorism in mind.

The Department is currently reviewing staffing levels in other areas that may have been neglected including counterintelligence, dignitary protection, and domestic facility security which continue to be significantly understaffed and underfunded.

Let me describe to you the universe of our efforts. We are in the protection business. We protect people, facilities, and classified information. We do this at our posts throughout the world.

Let me give you some idea of the magnitude of our global life safety responsibilities. We protect approximately 10,000 State Department employees in the United States. Overseas, we are accountable for the protection of an estimated 75,000 U.S. citizen employees and their families. Add to that number more than 37,000 Foreign Service employees working for our embassies and consulates. Each year we also protect approximately 130 distinguished high profile foreign visitors to the United States and that is an encapsulated view of just our mission to protect people.

Mr. Chairman, in my view the breadth of this global mandate is unique in the Federal Government.

Our missions for protecting facilities and information equally demanding. DS has designed programs to counter a global array of security challenges presented by elements ranging from common criminals to terrorists and spies. Our programs include safeguarding classified and national security information, personnel investigations, computer and information security awareness programs, and the conduct and coordination of espionage and counterintelligence investigations.

In the past year, much has been made of security incidents at Main State. Providing security for that building is a problem, not impossible but still very challenging.

The Department of State building is the second largest government building in the Nation's Capital. It is occupied by 8500 employees and receives over 200,000 official visitors and tourists each year. The Main State building covers two square blocks and has eight stories and a basement. There are 2.6 million square feet of space. It has 5 pedestrian entrances, 3 basement entrances to a 900 plus vehicle garage, 2 loading docks, 43 elevators, 5,400 windows, 9 acres of roof, and 13 emergency generators. The building has virtually no setback from the street thus affording little opportunity to screen either visitors or vehicles at appropriate distances.

The building serves as the hub for American diplomacy. It hosts numerous international conferences and major events involving world leaders each year. The building is the platform for the Nation's daily press briefing on events around the world. It houses the Nation's State dining rooms and unrivalled collection of colonial and early Federal decorative priceless art objects insured for $100 million.

The Department has in place procedures and safeguards to protect our facilities during construction and renovation. As this Committee is aware, Main State is currently undergoing a major 10-year renovation project. Security measures such as the development of construction security plans, construction surveillance, vetting of workers, screening of materials, and other precautions are integrated into this project. Other construction projects performed within the building are routinely scrutinized by DS officers to determine the level of sensitivity and ensure that proper security countermeasures are utilized.

In other words, the State Department building is a very large and busy institution. Protecting it is an immense challenge.

Three incidents in the Main State building have brought home to all of us the need to strengthen domestic information security. In February 1998, an unknown male in a tweed coat carried away classified documents from the Secretary's suite of offices. That case, which was investigated by the FBI, is in an inactive status at this time.

The second incident came to light on December 8, 1999 when Russian intelligence officer, Stanislav Gusev, was arrested on the street outside the State Department as he listened in on a meeting in the State Department's Oceans and International Environmental Scientific Affairs' conference room via a bug planted in the chair railing. Gusev, who had diplomatic immunity preventing his prosecution in the United States, was asked to leave the country. The investigation by the FBI continues into, among other things how the bug was planted. Spinning off the bugging case was an inquiry into how a computer software contract was managed and whether the systems on which the software was placed had been compromised. That inquiry is still ongoing.

The third incident is, of course, the laptop incident which is currently under investigation by the FBI and DS. Ambassador Roy has already described for you how the laptop was used, the circumstances surrounding its disappearance, INR's referral of this

matter to DS and the Secretary's five point response to the incident.

Mr. Chairman, we have learned some very valuable lessons from these incidents. The fundamental problem which has brought the Department to the point at which it now finds itself is not an absence of proper policies and procedures, as those are and have been in place. The problem is simply carelessness. That is, noncompliance and/or disregard for established regulations. These incidents have prompted us to take measures which complement existing regulations and procedures and are designed to change the lax attitude toward security at the State Department.

I believe that substantial progress has been made over the past 2 years. We have tightened security in the Secretary's suite of offices. We have adopted a rigorous, comprehensive escort policy, worked to strengthen computer safeguards, and assigned uniformed officers to floor specific patrols inside the building. At Main State we have reinstated an after-hours inspection program of Department offices, and we continue a program of bringing Marine security guards in training into the Department 10 times a year to conduct security sweeps. We have closed D Street outside the building to traffic and installed cement barriers around the entire building, thus lessening our physical vulnerability. We have provided security awareness briefings to over 4,000 Department personnel. But these are only the first steps. Much more needs to be done.

In March, I convened an interagency review panel comprised of senior security representatives from the FBI, the Department of Defense, the U.S. Secret Service, the CIA, and the Diplomatic Security Service. The panel was asked to review the countermeasures currently in place to protect against unauthorized access to the Main State building and classified information. I also requested that they make recommendations to improve security at the Main State building.

On Monday of this week, I received the panel's report. I plan to present the report to the Secretary when she returns to Washington and intend to use it to correct systemic vulnerabilities at the Department of State. Once the Administration has had an opportunity to review the report, I will be delighted to share it with you, Mr. Chairman, as well as the Members of your Committee.

This panel confirmed our assessment of known weaknesses in our programs and recommended both short and long term solutions that it believes will enhance security at Main State. Their findings center on Main State's access controls, its physical security, information security, security awareness, our uniformed protective officer program, and the need to create a chemical/biological program. I am convinced that the development of a strategic plan to fund and implement these findings will result in significant improvements in our programs.

The Secretary's leadership in raising security awareness has been invaluable. She has personally emphasized security at every opportunity for the purpose of strengthening the culture of security at State. As you know, on May 3 she held a Department-wide town meeting on security because of the laptop incident. In the course of the meeting, she stressed that each of our employees must be our neighbor's keeper when it comes to security. The position that

she has taken with respect to individual responsibility among our diplomats, that regardless of how skilled you may be as a diplomat, if you are not professional about security—you are a failure—has resonated throughout the Department. Further, when she told the Department employees that the press reports were accurate; and she was indeed furious about our security lapses, any misgiven belief anyone might have that the Secretary wanted simply to let this blow over and be forgotten was forcefully corrected.

I believe that what we have done and are doing, combined with the stark ugly reality of what security failures produce, have gone a long way in raising awareness at the Department. I think that we have reached the point that where the decided majority of State Department employees has recognized that a threat exists; that poor practices are unacceptable; that security is a high priority with the Secretary, this Administration, and this Congress; and that employees will be held accountable for lapses. I can assure you that the Secretary and I will continue to drive home those points as forcefully as possible.

As I said earlier, I believe that the lax attitude in the Department toward security is no longer tolerable. I fully expect that we will see that the Department's efforts aimed principally at better education, at existing requirements, and designation of individual responsibilities will bear fruit and there will be substantial and voluntary adherence to security rules and procedures, but if I am wrong, we are fully prepared to use enhanced disciplinary procedures to further underscore the seriousness with which we view this issue.

Thank you, Mr. Chairman. I would be glad to answer questions at this time.

[The prepared statement of Mr. Carpenter appears in the appendix.]

Chairman GILMAN. Thank you, Mr. Carpenter.

Mr. Bereznay, section chief, National Security Division, Federal Bureau of Investigation. You may summarize your statement, or your full statement will be made a part of the record, as you deem appropriate. Please proceed.

STATEMENT OF TIMOTHY D. BEREZNAY, SECTION CHIEF, NATIONAL SECURITY DIVISION, FEDERAL BUREAU OF INVESTIGATION

Mr. BEREZNAY. Thank you, Mr. Chairman. Members of the Committee, I am pleased to appear before you today to discuss State Department security issues that are of concern to this Committee. I will be as forthcoming as possible given the sensitive and classified nature related to the information requested by the Committee.

Concerning the missing State Department laptop computer, I want to ensure the Committee that the FBI's investigation of the missing computer is being afforded the highest FBI priority. As you are aware, I am prohibited from discussing the matter further as it is the subject of a pending criminal investigation.

The Committee has asked that I comment on the sufficiency of State Department security procedures in connection with the bugging of the 7th floor conference room by the Russian Foreign Intelligence Service. The FBI was asked by State Department in late

August 1999 to conduct an environmental technical survey, in other words a review of neighboring properties, to determine whether a hostile intelligence service might have acquired such property. This survey was specifically requested in connection with pending renovations at the Department. In 1998, we were also pleased to have our Washington field office work with the Office of Diplomatic Security to survey access to State Department by Russian intelligence officers. Beyond these narrow surveys conducted with or at the request of State Department, the FBI was not called upon at that time to review physical security procedures at the Department. Those matters were, however, addressed by the Office of the Inspector General as reported in its September 1999 report.

The FBI believes that the State Department acted swiftly during August 1999 to limit the number of unescorted foreign nationals visiting State Department following the discovery of the listening device in the 7th floor State Department conference room. On August 23, 1999, the State Department implemented policy that requires all foreign nationals to be escorted within the building at all times.

As noted by the Committee, there is an exception for foreign media correspondents issued unique but permanent badges that allow unescorted entry without passing through metal detectors.

There is an understanding that the media is not to go above the second floor where the press office is located. This exception affords unescorted access to the State Department by a number of known foreign service intelligence officers. The FBI does not customarily provide other agencies, to include State Department, with lists of intelligence officers' identities to protect both sensitive sources and cases unless there is a specific reason or if asked. If asked, the FBI would be willing to identify to the State Department permanent media badge holders identified as hostile intelligence officers so that their access could be restricted or their visits monitored.

Historically, hostile intelligence services have utilized media cover for intelligence activities in the United States. However, because intelligence officers under media cover do not have diplomatic immunity, they normally perform in-depth but overt intelligence collection. Clandestine handling of agents or other covert activity is usually assigned to intelligence officers under diplomatic cover. In addition to the overt intelligence collection, intelligence officers under correspondent cover have been engaged in active measures campaigns designed to support their national interests and to influence United States policymakers.

Active measures campaigns take the form of oral persuasions or the dissemination of written information favorable to their national policy, both of which are facilitated by intelligence officers under media cover. Hostile intelligence services use active measures as an inexpensive and relatively low-risk way to advance their international positions.

Over the last 15 years, no foreign intelligence service officer under media cover has been declared persona non grata for engaging in espionage activities. This is attributed, as I previously noted, to the fact that these officers are not accredited diplomatic immunity and thus normally do not engage in clandestine agent-handling activities subject to interdiction.

With respect to your inquiry regarding the use of laptop computers within the FBI, the FBI uses only specified laptop computers that carry appropriate safeguards for classified data, to include both the use of passwords and encryption. These laptops are maintained by automation personnel and are available for short period loans to FBI employees. The laptop computers are periodically examined and the stored information purged. When they are turned in by one employee and before being issued or loaned to another individual, the hard drive is purged and reprogrammed. The laptop computers are also subjected to an audit and forensic check to ensure that they have not been compromised.

The FBI views the protection of classified information in a computer environment as a problem that is not unique to the State Department. It is a serious security issue that will continue to present problems to all members of the intelligence community.

I welcome any questions you may have.

[The prepared statement of Mr. Bereznay appears in the appendix.]

Chairman GILMAN. Thank you very much, Mr. Bereznay, and I want to thank our panelists for their testimony. We will now proceed with questions.

Ambassador Roy, in your statement, you note that there are appropriate procedures for management's security of renovation projects in secure areas of the Department. The question is, were these procedures followed in the renovation project that took place in the INR suite on the sixth floor?

Mr. ROY. Mr. Chairman, the investigation will determine the exact circumstances relating to that. What I can do is share with you my understanding of what happened.

Chairman GILMAN. Well as you share it, can you tell us, did the construction plan permit uncleared workers to be in the classified area and permit the door to the hallway be open during the work day? Can you also note the dates of the renovation project for us?

Mr. ROY. Yes. The construction workers were expected to be escorted at all times and the appropriate instructions were given to the office where the construction work was taking place. At no time was there unsecured access by the workers to the controlled areas of the SCIF. When the door was opened in areas of the office that were being renovated, either access had not been broken through the wall to make it part of the SCIF or there were people stationed at the entrance in order to provide protection. The procedures were expected to be followed and were consistent with our understanding of appropriate DCID directives.

Chairman GILMAN. Who is responsible for assuring that the repairmen were escorted at all times?

Mr. ROY. The office where the work was being undertaken were charged with that responsibility.

Chairman GILMAN. So whoever was working there would have to make certain they were escorted?

Mr. ROY. Yes.

Chairman GILMAN. And it is also our understanding that INR employees were tasked with watching the workers. Did it make sense to have employees who had their regular assignments also have to watch these workers?

Mr. ROY. The workers had to be watched, and if INR employees were charged with that responsibility it should have been carried out. My personal view is that in situations like that you need dedicated people who have a 100 percent responsibility of monitoring the uncleared workers. That is the ideal way to accomplish it.

Chairman GILMAN. How adequate was the oversight of the workers at the time of the renovation project?

Mr. ROY. Most of this occurred before I arrived in INR so I cannot speak from personal experience, but what I can share with you, Mr. Chairman, is the fact that I have never been permitted access to INR work spaces as an ambassador, as the executive secretary of the Department responsible for document flow to the Secretary of State, as a deputy assistant secretary of a geographic bureau in any other way than an escorted manner.

Chairman GILMAN. And who did the escorting?

Mr. ROY. INR employees. Every time that I, as a foreign service officer not working in INR, have been to INR spaces, I have been escorted 100 percent of the time. So my expectation was that the escort duties were taken seriously.

Chairman GILMAN. Mr. Carpenter, who is responsible for security of a renovation project at the Main State building particularly with regard to projects that take place in classified areas?

Mr. CARPENTER. In our domestic operations section there is actually a differentiation between the rest of the building and INR space. For anywhere else other than INR space and SCIFs and the like, INR had that responsibility for the rest of the building, our domestic office.

Chairman GILMAN. Who is in charge of the domestic operations office?

Mr. CARPENTER. Don Blake.

Chairman GILMAN. Are there security-oriented regulations that govern such construction of renovation projects at the Main State building?

Mr. CARPENTER. Yes there are.

Chairman GILMAN. Are the regulations different from the rules followed for overseas construction for the protection of sensitive areas?

Mr. CARPENTER. Yes they do differ yes, sir.

Chairman GILMAN. In what manner?

Mr. CARPENTER. Overseas are much more stringent by virtue of the potential for compromise as construction is going on. They are also dramatically more stringent.

Chairman GILMAN. Do you think there should be more stringent regulations here in the Main State building?

Mr. CARPENTER. Absolutely.

Chairman GILMAN. If work will occur in a classified area, can uncleared workers be used?

Mr. CARPENTER. Uncleared yes, unescorted no.

Chairman GILMAN. Does diplomatic security provide security technicians for such projects?

Mr. CARPENTER. Occasionally, depending on the amount of notice we are given and the availability of our personnel.

Chairman GILMAN. And could INR have requested escorts from DS who are trained to watch workers?

Mr. CARPENTER. I suppose they could have requested that. Again, the security of their areas is largely—has previously been—their responsibilities.

Chairman GILMAN. Ambassador Roy, until the recent announcement—you were responsible for the directives governing the SCI material, is that correct?

Mr. ROY. That is correct.

Chairman GILMAN. Have you been able to determine whether the laptop computer was used in accordance with the Director of Central Intelligence directives?

Mr. ROY. Yes, sir. My understanding is that it was used and stored in consistency with the pertinent directives.

Chairman GILMAN. Are there regulations governing labeling or requiring encryption or even a password to protect information stored on a laptop? Are there such regulations?

Mr. ROY. There are regulations concerning labeling. My understanding, and we have looked at this in retrospect, is we cannot confirm with assurance that there were appropriate labels on the laptop, although some people have told me that they recall seeing such labels on it.

Chairman GILMAN. Are there now labels being required on a laptop?

Mr. ROY. Yes, there are.

Chairman GILMAN. Ambassador Roy, were your employees abiding by the proper visitor escort procedures in the INR office where the laptop was lost?

Mr. ROY. Since the laptop is missing, there had to be a lapse somewhere, but insofar as I was aware they were abiding by the procedures and they were certainly informed of what the correct procedures were.

Chairman GILMAN. And Ambassador Roy, has anyone been held accountable for the loss of the laptop?

Mr. ROY. That is not possible, Mr. Chairman, until the investigation is concluded.

Chairman GILMAN. Any disciplinary action under way?

Mr. ROY. No disciplinary actions have been taken pending determination of responsibilities.

Chairman GILMAN. And, Mr. Carpenter, in November 1998, you introduced, with the approval of the Under Secretary for Management, a policy requiring escorts for many State Department visitors. Within a week, that was rescinded; and later in August 1999, following a discovery of a bug in a conference room at State, the requirement for an escort was reintroduced. Can you tell us who requested the rescission of that order?

Mr. CARPENTER. Yes, sir. As you properly stated—I answer to the Under Secretary for Management. Almost immediately upon arriving at the State Department, realizing that there was no escort policy for anyone, quite frankly, to enter the building, we started to put together a program. We briefed the Department as fully as we could relative to how it would work. As you said, in November, I submitted it to my under secretary.

Chairman GILMAN. November of what year?

Mr. CARPENTER. Of 1998.

Chairman GILMAN. Yes.

Mr. CARPENTER. My under secretary approved; we proceeded in issuing fliers about this new program. I was called within hours of it being distributed by Under Secretary Pickering. He asked me to explain exactly what was going on. He had not been briefed on it. A number of the people that answer to him in the geographic bureaus claimed not to have been briefed on it. It appeared to be that it was a policy that had never been instituted at the Department of State. People felt it would be too confining and it wasn't doable and asked me to withdraw it.

Chairman GILMAN. Who asked you to withdraw it?

Mr. CARPENTER. Under Secretary Pickering. We went back to the drawing board. We conducted more briefings. We, quite frankly, made the escort policy better. We did some marketing—people better understood what needed to be accomplished. We talked to those people who were most concerned, people that would be entertaining large groups, how that would work. Some of that work, quite frankly, had not been done.

Chairman GILMAN. When did you reintroduce that?

Mr. CARPENTER. In August 1999, less than 1 year ago.

Chairman GILMAN. And has it been in place since August 1999?

Mr. CARPENTER. Yes, sir, it has and working quite well.

Chairman GILMAN. And, Mr. Carpenter, one of the concerns in the current escort policy is the exception for the press corps. Understanding they are supposed to be restricted to the first two floors of the building, what is to prevent them from moving about freely in the other floors?

Mr. CARPENTER. Currently, we realize that the press and their ability—the answer to your question is nothing at the current time prevents them from going to other floors.

Chairman GILMAN. So they have free access now.

Mr. CARPENTER. They do not have free access. They are instructed that they are not to go above the second floor. We have guards patrolling the floors, second, third, fourth, fifth, sixth, etc., looking for not only press who are unescorted but other people who may have left an office without escort.

Chairman GILMAN. Unless they are confronted by a guard, they can wander around the building; is that correct?

Mr. CARPENTER. It would be possible. Yes, sir.

Chairman GILMAN. Can you tell us how you issue press credentials to the American/foreign press? Is there any distinguishing process between the two?

Mr. CARPENTER. Yes. There are checks that are made and probably this would not be the forum I would want to go into what those checks are, but clearly there will be checks done on them.

Chairman GILMAN. As part of your new escort policy, are random hallway checks done to identify persons not eligible to be wandering around a building?

Mr. CARPENTER. Yes, sir. They are.

Chairman GILMAN. I know I have exceeded my time but this is such an important issue. To our FBI assistant, since the chair-rail incident, has the State Department done everything it can to minimize security problems and threats, in your opinion, to the Main State facility?

Mr. BEREZNAY. As I indicated in my statement, Mr. Chairman, since that incident, there has been a tightening of the escort policy. The only area where I see a need for improvement is one you have already addressed, that being foreign media correspondents' access at State Department.

Chairman GILMAN. Does the gentleman's agreement that badged foreign press officials remain only on the first two floors of the State Department unless they are escorted pose any serious security threat?

Mr. BEREZNAY. In my opinion, it poses a threat. Realizing that those media representatives could be working in conjunction with other visitors from foreign countries, I believe that there is a threat there. As I indicated, we would be willing to work with State Department to identify those journalists—foreign journalists who we know to be intelligence officers so they can be either more vigilant during the visit or restrict those visits.

Chairman GILMAN. To your knowledge, are there foreign press representatives who are intelligence officers now serving in the State Department?

Mr. BEREZNAY. Mr. Chairman, yes, there are.

Chairman GILMAN. Thank you. Ms. Bridgers, does the escort policy raise any concerns with your office.

Ms. WILLIAMS-BRIDGERS. Yes, Mr. Chairman, the escort policy does raise a number of concerns, specifically those that you have just focused your attention on within the past few moments. We believe that the escort policy as written is an excellent first step in controlling visitors to State Department, but it does leave a glaring hole in allowing the press, members of the media, free access to the building.

Chairman GILMAN. Thank you. Mr. Gejdenson.

Mr. GEJDENSON. Thank you, Mr. Chairman. Let me just start on the computer. Do you need to have a laptop, I mean, was there a reason for it to be a laptop.

Mr. ROY. Let me address that, Mr. Gejdenson. The laptop was acquired through funds provided by the intelligence community because officers working on non-proliferation issues, outside of INR, did not have secure computers within INR that they could do their work on. The information had to be stored in INR. For that reason, a laptop was purchased with intelligence community funds in order to have a workstation available within INR that could be used by cleared employees from outside of the Bureau who needed to work on SCI material within INR.

Mr. GEJDENSON. Was there a need for the computer to be mobile or could the same things have been accomplished by having a full-size desktop?

Mr. ROY. In principle, it could have been accomplished by having a full-size desktop and eventually——

Mr. GEJDENSON. Just because it is harder to steal and larger——

Mr. ROY. To be frank, the idea that either a laptop or dedicated workstation could have been stolen was not driving the decision.

Mr. GEJDENSON. I understand that, but in the field which you are, when we take a look at getting a system for outside people who are coming to State, we could simply get a desktop instead of a laptop. They could still steal the hard drive. There are lots of

ways to steal information. You can download it, send it over a modem, but physically it will be harder to remove it if it is not a laptop in the future. So that may be one of the things you ought to look at is whether or not you need to get smaller systems or whether you need to encase them in larger systems just as an additional security measure.

Mr. ROY. I agree with you entirely; and in practice, INR laptops are only used for those mobile situations where only a laptop can be used. In other cases, we use dedicated workstations.

Mr. GEJDENSON. Mr. Carpenter, do you have enough authority? My sense from your answer on the escort issue is you had to learn the politics of the State Department so you worked it through. Like any institution, institutions don't like new people who come in and change the way they have lived. It has worked fine before you got here. You tried something, you did a pretty good job, but obviously then you had to sell it, refine it, as you said. You should be a diplomat, you are very good at these things, but basically putting aside the need in any institution to learn how to move things along, do we need to change the structure in any way so you have the authority necessary to take the actions you consider important in an expedited and timely manner?

Mr. CARPENTER. Well, they didn't hire me to be a diplomat. I think State hired me to look at the security issues with the eye that needed to be focused on them. The Secretary has been incredibly supportive of the efforts that we have made to try to improve the security at State. The issue that was addressed earlier about the escort policy, we were clearly aware of a hole that is there. There are steps that have been taken to mitigate those holes, and I will be glad to discuss those again in another forum.

Your statements about the need to be diplomatic—we could not be. The State Department had never had an escort policy, never or anything close to it. It was very, very difficult to drop the curtain on the Department. It had all sorts of ramifications—so we had to do it in phases. This is simply the first one. Are there holes in it? Absolutely. We are looking at such things as hiring permanent people that do nothing but escort. We are looking at converting different parts of the building to secure or nonsecure areas only, to better facilitate the conduct of our foreign affairs. There are a number of things that need to be done. As the Inspector General mentioned, this escort policy was only a first step.

Mr. GEJDENSON. Do you have authority enough in the structure of the State Department? This is an old system, a lot of people around, lots of power centers under the present construct, whether it is you or anybody else there. Do you have authority to move forward and do the things that need to be done at the Assistant Secretary level? Or do you need a different title or more staff? Are there any of those things?

Mr. CARPENTER. I am glad you asked. The Secretary is working with Congress to establish, as soon as possible, a new position for Under Secretary for Security, Counterterrorism and Law Enforcement. The genesis of this concept was from the accountability review board following the East Africa bombings that suggested that the Department of State needed to designate one person to be re-

sponsible for all security issues at the Department of State. This position clearly does not exist.

The question that was posed is—at what level does that person have to be to function. Currently, I have what you would call an informal reporting to the Secretary herself. I brief her every morning. That certainly gives me a certain profile, but I also answer to the Under Secretary for Management. There are other elements in the Department that from time to time address security issues. The Department is full of security experts from time to time. I think it is important that security issues be resident under one person so that this body and the Department of State in total understand who is responsible. I think this would be an excellent step.

Mr. GEJDENSON. Now, and you kind of mentioned this, but you sense there is a need to change the operation of the physical plan so some areas are basically sealed off to the public, no access unless you know a code or some kind of card entry. We are using all the modern technology that is available today to both limit access to rooms and to have a record of who enters and leaves a room. For instance, where this computer was, do we know everybody who entered and left that room.

Mr. ROY. Yes, we do.

Mr. GEJDENSON. And so somebody who entered and left that room must have taken the computer, there is no one else that could have done that.

Mr. ROY. No, sir.

Mr. GEJDENSON. Now let me ask the gentleman from the FBI. My instincts are that State needs these internal services and somebody at a level appropriate to oversee them. Is there any argument that says we should have the FBI do this? It might cause a little interagency tension, not that that ever happens much in Washington, but maybe having an outside agency watching the security on a regular basis might be more effective, is that your view?

Mr. BEREZNAY. I don't believe that the FBI should be asked to do that sort of function, for the State Department or for any other agency. I think that State clearly has the ability through the Office of the Inspector General and diplomatic security to undertake those functions.

Mr. GEJDENSON. And Mr. Carpenter, if we know that some of the foreign press that are at State are collecting information for governments, friendly or unfriendly, to the United States, wouldn't it make sense to immediately secure the other floors from their—I mean, if I was a reporter for another country, is it possible for me to walk in the elevator and push a button and go to a floor that I shouldn't be on or walk up a hallway that I shouldn't be in.

Mr. CARPENTER. It has been made more difficult but clearly not impossible.

Mr. GEJDENSON. And so shouldn't we have some, again, system by which they physically can't get there? So it is not just their good intentions and our, you know, people in the hallway spotting them but that it is physically impossible for them to open doors they shouldn't open.

Mr. CARPENTER. Congressman, as I said previously, I am not a diplomat. I was hired to be a security officer. If it was within my

power, I would not have the press actually in that building. I would have them offsite somewhere we could more easily control.

Mr. GEJDENSON. That is not a bad idea actually. So you would have the press outside the actual State Department building physically.

Mr. CARPENTER. It would be much easier, either outside the building or confined to a lower floor area where they would have access only, much less access.

Mr. GEJDENSON. So when they were invited in you could let them in. The rest of the time you keep them corralled. I like that approach for here as well.

Now what about the report that the door was being propped open while people were working there? Is that correct?

Mr. ROY. Let me give you my understanding of the circumstances.

The office in question was having an adjacent office altered to become part of the office. At the time that the alteration work began, they were not connected. They were contiguous to each other, but they were not connected. There were separate access doors to the new office space. During the period that that new office space was being renovated and before it had been added to the office in question, the door was sometimes propped open so that the workers could gain access.

Mr. GEJDENSON. But at that point there was no entry from that space to the secure space?

Mr. ROY. Correct.

Mr. GEJDENSON. And there was no secure information in that space?

Mr. ROY. Correct. And following the knocking through of access to the office in question, the passageway was monitored full time.

Mr. GEJDENSON. So what we have is we have a laptop missing from a room. If you open that door and I walked in with you, where would be the record that I was with you?

Mr. ROY. That particular office did not have a log-in/log-out procedure at the time, so that you would be under the responsibility of the person escorting you.

Mr. GEJDENSON. So no one could enter the room without somebody authorized escorting them. But if somebody—if a friend of mine worked there and I walked in with him and he didn't note that I was him at any point, then——

Mr. ROY. The procedures followed were that you had to be under positive escort. I myself as Assistant Secretary could not gain access to the office because I did not know the door combination, and you could not gain access without being either admitted by somebody from inside or knowing the combination.

Mr. GEJDENSON. So if somebody took you in there, was there a record of your presence?

Mr. ROY. No, sir, not at the time.

Mr. GEJDENSON. So we have everybody who has entered, but not everybody who accompanied them, and that is the rub.

Mr. ROY. Once you were inside, you had to be accompanied——

Mr. GEJDENSON. Right.

Mr. ROY [continuing]. And the personnel in the office were indoctrinated to determine whether you had an SCI clearance or not when you were admitted to the space.

Mr. GEJDENSON. Now on the gentleman in the tweed jacket and the question there is, whose responsibility is that? Mr. Carpenter, you weren't there yet, but that would go under your responsibility now?

Mr. CARPENTER. Yes, sir, it would.

Mr. GEJDENSON. And basically what happened was there was a file left out in the receiving room.

Mr. CARPENTER. There were a number of files set on a desk between two secretaries.

Mr. GEJDENSON. And a gentleman came up, looked at the files, took some things. And that floor—was that a secure floor?

Mr. CARPENTER. Yes, it is. It is the Secretary's suite. The Secretary was not in at the time, I might add.

Mr. GEJDENSON. If I come to the State Department, first I have got to get past those lines. So if I am a reporter, I could get through and go unescorted to my press area, but I could also go up in the elevator to the Secretary's floor.

Mr. CARPENTER. To the Secretary's floor but not the Secretary's suite.

One of the things that probably will clarify some of this, the person that took these was believed to have a State Department pass, wearing a State Department pass, which allowed them access through their card swipe into her suite of offices. Unfortunately, as Murphy's law would take place, the day that this was done, the system that read who came in was down.

Mr. GEJDENSON. That was a coincidence, you think, not intentionally done?

Mr. CARPENTER. We see no evidence that it was intentionally done. Nothing to indicate that.

Mr. GEJDENSON. So as one of the things—and my time's up here—do we need to look at something that, whether it uses, I don't know, the thumbprint, eye scan, I mean, this is the most important information we have as a country. It seems to me we have to have much more positive information on who enters and leaves rooms, and I shouldn't just be able to give somebody else my card to allow them access. Are you looking at all that?

Mr. CARPENTER. Yes, sir, we are. As a matter of fact, we are in the process of purchasing a system for access, not only to Main State but other critical areas, that is a combination of a card swipe identifier as well as a redundant pin system like used in most places throughout this city.

Mr. GEJDENSON. What I suggest is—and I know the Congress has not been supportive of the President's and the State Department's request for funding and we have kept the pressure on you in trying to cut—that incidents like this give you an opportunity to get what you need. What I would suggest is that you ask for a supplemental amount of money—segregated funds based on our security needs at State and other facilities around the country—and that you get that up to us as soon as you have it.

You better be able to defend it. But it seems to me we have got lots of crises to respond to—we have wars, we have got starvation.

We have had some trouble in this area in the past, but I think you ought to hand up a supplemental request for security. Make sure the systems we need are there, here and around the country. Obviously, that is going to include training personnel, because just having the system without changing culture and training isn't going to work.

Thank you, Mr. Chairman.

Chairman GILMAN. Mr. Rohrabacher.

Mr. ROHRABACHER. Thank you very much.

You know, I have been trying to get some documents out of the State Department for about 2 years. I must have been asking the wrong guys to get it for me. Let me get this right. I really have. I should have asked some of those intelligence officers over there.

Mr. Roy, let me get this straight. We have had a policy where you have to be escorted, but we have the FBI telling the security people here that we have got intelligence agents posing as members of the press who are running around the building unescorted. Something's screwy here. Am I missing something?

Mr. ROY. Let me just make a very quick response to that.

We have special additional procedures in INR required by the Director of Central Intelligence Directives. These procedures go beyond the general ones that apply to the State Department as a whole which is under a different security regime.

Mr. ROHRABACHER. I don't know if that was an answer to my question or not. It sounds like the answer to my question is that you have testified here today that you can't go unescorted and the FBI's already testified that they have complained that we have intelligence agents posing as reporters running around the building unescorted.

Mr. ROY. Let me quickly clarify I am not escorted when I wander around the State Department. When I was not working in INR, I was escorted when I entered INR secure spaces.

Mr. ROHRABACHER. All right. It sounds like, to me, that at times you have had to have escorts and foreign intelligence agents haven't. But that is a matter of—I don't know how important that is, but it just seems to suggest that things are out of whack over there.

By the way, when things are out of whack, there is always testimony by someone, let us just hire a czar. In this case, it is going to be a new under secretary.

According to the reports that I have seen, the State Department now has more money, taking inflation into account, than it has ever had for internal operations which could have been directed by the Secretary or the White House to be spent for these security reasons. Isn't that right? So we are not talking about lack of money here. You have got more money than you have ever had before, but yet we have these situations.

How is hiring on a couple new employees at very high prices going to change that? This is an attitude problem. This isn't a lack of personnel. This is what I am hearing here, and it is real easy to try to think that we are going to solve problems by creating a new under secretary for this or that. It seems those problems never get answered.

Let me put it this way. From an outsider—and I want to just look at this from a broader perspective. I think this Administration has had a lax view toward national security and toward these intelligence concerns from day one.

There was a book by Aldrich Ames called Unlimited Access about the security violations that started almost immediately after this President became President of the United States. If you have an attitude from the White House which ends up permitting the transfer of massive amounts of technology to the Communist Chinese as well as—obviously, an attitude in this White House, where you have campaign contributions flowing into funds and then we find out that—coming from the people who produce missiles and rockets in Communist China, and we found out that there has been problems with a transfer of technology, of course people down the ladder are going to have a lax attitude toward national security matters.

Let me just get down to a specific, to our FBI man. The FBI complained that there was access to the State Department by foreign intelligence officers posing as reporters. That is what you have testified today, is that correct?

Mr. BEREZNAY. That is correct.

Mr. ROHRABACHER. OK. That was very clear in your testimony. When that complaint was made, what was done to act upon that? Was there something?

Let me ask Ms. Williams-Bridgers.

Ms. WILLIAMS-BRIDGERS. In the course of our audit looking at the handling of classified information, we asked to obtain a copy of the FBI report that alluded to foreign intelligence officers operating under cover of press, and we were denied access to that report. So this is the first that I am hearing today a positive affirmation that there are media who are, in fact, intelligence officers operating in the Department.

Mr. ROHRABACHER. OK, so we have got to find out what happened today. But, you actually in your job of trying to investigate this didn't have that information.

Ms. WILLIAMS-BRIDGERS. We did not, sir. That is correct.

Mr. ROHRABACHER. Well, this is——

Chairman GILMAN. Will the gentleman yield?

Mr. ROHRABACHER. I certainly will.

Chairman GILMAN. When did you learn about the report by the FBI?

Ms. WILLIAMS-BRIDGERS. We learned about it during the course of our audit which was conducted between August 1998 and September 1999.

Chairman GILMAN. Who did you make the request to for that report?

Ms. WILLIAMS-BRIDGERS. To the FBI. I am not certain of the exact name of the individual or the unit, but our audit team did request a copy of the report, and we were told that we would not be allowed to see it.

Chairman GILMAN. Did you followup that report with the Secretary of State to make a request of the Secretary?

Ms. WILLIAMS-BRIDGERS. No, we did not, sir.

Chairman GILMAN. Thank you.

Mr. ROHRABACHER. Let me correct the record. It was Gary Aldrich who was the FBI agent who wrote Unlimited Access and not Aldrich Ames, who was a spy who has probably applied for press credentials over at the State Department.

Well, let's hear about it. Why wasn't this acted upon or was it acted upon? And why is it that the person who is supposed to be overseeing this, making sure problems don't happen, was not given a copy and even didn't know that this report had been made and this complaint by the FBI was present?

Mr. BEREZNAY. The report that is being referred to is a classified report, and it basically entailed a survey, a joint survey, that was done by the Bureau with Diplomatic Security. It was done in 1998, and it was done specifically to address the issue of visits to State Department by foreign intelligence officers.

Mr. ROHRABACHER. And was it acted upon? What happened to act upon this report? That is the question.

Mr. BEREZNAY. As a result of that I believe Mr. Carpenter has testified to the implementation of escort policies and the attempt to implement that and——

Mr. ROHRABACHER. But the escort policies have nothing to do with the media, right? I mean, is the media now—I thought what we were hearing here is that we still have a problem. The media still can go around that building unescorted.

Mr. CARPENTER. Let me try to clarify this. Can they—could they be there right now? Yes, they could.

The program is designed so that they can't—and, as I mentioned earlier, this is a vulnerability that we are well aware of, and there are things that we have done to mitigate that that I prefer not to go into in this forum. I would be glad to discuss it later because it does involve some other issues.

But the press, Congressman Rohrabacher, are not allowed unfettered access above the second floor. Since—in the last year since the escort policy has been in place, we have had seven incidents—excuse me, one incident of a press person caught above the second floor. It wasn't a foreign press, but that individual was picked up by our uniform people and promptly returned.

Mr. ROHRABACHER. I think the operative word there is "caught"—you know, caught.

Let me just say again, I don't think that we can, Mr. Chairman, I don't think that we can just wish and point our fingers and blame people at lower levels for having a lax attitude, which is what you have been describing today. There was been this lax attitude of security, and you are trying to do something about it. We can't blame that when we have got, at even the highest levels of this Administration, what I see as a totally lax attitude toward the national security and toward intelligence in the United States.

I mean, this Administration—considering all the transfer of technology and information that we have had to a potential enemy like Communist China, this Administration looks like a spaghetti strainer. When you go down—and the fact is they have known about it, we have known about it, and they make light of it. How can you expect people further down the line to take their job seriously when we have got this coming from above? I think that we need to change the procedures.

My hat's off to you for the serious way you are trying to do it. But it is going to require more than just hiring another high-level executive and putting another nameplate on the door. It requires a change from top to bottom in terms of people's attitude toward this country's national security.

One last statement, Mr. Chairman. That is, when we talk about laptops and we talk about documents that are missing, what we are really talking about here is the national security of our country has been compromised. Let us not try to minimize how important that is. People's lives are at stake with these national security issues. Whether or not in the long run people may lose their lives we will never know if it was due to information on that laptop or how the laptops work, getting into the hands of people who are enemies of our country. This is a very serious issue; and I appreciate you, Mr. Chairman, trying to take the lead and get the word out on this.

Chairman GILMAN. Thank you Mr. Rohrabacher.

Ms. Lee.

Ms. LEE. Thank you, Mr. Chairman; and thank you also for this hearing.

Let me just ask first just a general question.

In terms of trends, have you seen, I guess, an increase in security breaches since the end of the Cold War. Did the State Department have more stringent security procedures in place during the Cold War or how has our security sort of emerged or not emerged since the Cold War or since the end of the Cold War?

Mr. CARPENTER. I will try to speak to my knowledge—to the best of my knowledge since the end of the Cold War.

Clearly, during the Cold War and those periods prior to it, there was a—the perception that the majority of danger of either threats from espionage or some other type of penetration was primarily overseas.

The Department of State, again, had no escort policy in place in spite of the Cold War ending. The State Department has actually gone the other direction. We have instituted an escort policy. It makes no sense to have, whether they are Russians or other foreign visitors, visitors in the building unescorted. So we have taken a very strong position on this, albeit a radical change from prior periods of time.

Clearly, there is an upswing in the espionage activities. I don't know of any other Federal building that has been penetrated in recent memory by foreign agents in the way that the State Department was. I think that this clearly shows they have the capabilities, they have the will and the want.

Ms. LEE. So then would you say that security possibly has increased since the end of the Cold War but so have counterintelligence activities?

Mr. CARPENTER. Put another way I think I am saying that those involved in the mitigation of counterintelligence activities have always understood the threat, have always been forward leaning on this as well as people charged with the security of buildings, the security of individuals and classified information. But, quite frankly, in the absence of the smoking gun, sometimes it is difficult to get the funds that are required in order to do that promptly.

Ms. LEE. Mr. Chairman, let me just ask another very quick question.

Now, the loss of the laptop and the tweed jacket and listening device incidents all reflect major failures in the security system, but now do you think that—without breaching security, do you think that these are isolated incidents or do you think that the dots could be connected? I mean, do you think that there could be some actual organized counterintelligence activities going on or, again, are these isolated incidences unto themselves?

Mr. CARPENTER. At least two of the incidents, two of the three, the tweed coat and the INR laptop, I would say to be examples of individual failings, carelessness on the people's part. The tweed coat—the information taken by the gentleman in the tweed coat was taken right out from between two individuals who did not report it in a timely fashion or this individual probably would have been able to be apprehended. The accountability again, the carelessness, and the laptop is an individual failing. I don't think security people are in the position of making judgments whether this is—I think your word was a trend or a—I am sorry, Ms. Lee.

Ms. LEE. Well, in terms of the second part of my question, are there any type of organized counterintelligence activities going on or are these isolated incidents as you see them.

Mr. CARPENTER. We don't see these as isolated incidences. We see these as ongoing problems with people intent on finding out our secrets.

Ms. LEE. I think as we look at the structure and move toward trying to make some major systemic questions, because that is what it sounds like, I would hope that if we do have another office or another unit responsible for and activities and security initiatives become part of the entire culture and that we don't hone in on just a few new departments or agencies or under secretaries isolated from the entire State Department. Because if that's the case, we will have really not done what I think we need to do.

Mr. CARPENTER. I couldn't agree more. We are not trying to create something new here. We are trying to take advantage of the synergies that are between existing bureaus within the Department of State and combine them under one person who can oversee these issues. That way we gain the values and the efficiencies of having, in this particular case, the diplomatic security bureau that I represent, the Office of the Coordinator for Counterterrorism and the Office of International Narcotics and Law Enforcement, combined under one. We are just trying to put together the organizations, bureaus, and offices that already exist and take advantage of that.

We think that security has to be core to the Department of State and, to that end, it is location, location, location. And as the security elements within the Department are currently positioned, we are not gaining its full advantage. That is what this proposal for an under secretary is geared to accomplish.

Chairman GILMAN. Thank you Ms. Lee.

Mr. Smith.

Mr. SMITH. Thank you, Mr. Chairman. I apologize for missing most of the testimony, although I have read some of it. We had markup going on up in Veterans on the GI Bill of Rights, and I just

could not leave it until it was finished. Let me just ask a couple of questions.

Obviously, it is the sensitive information in the laptop or perhaps laptops that matter, although the financial loss of any Department asset obviously should be something that concerns us. But obviously, again, the highly sensitive nature of the secrets, the fact they can compromise our personnel overseas and do a whole host of damage to our national and international interests makes that information beyond the price—priceless, if you will.

I wonder if you can tell us what are the security procedures in place and perhaps even contemplated to ensure that secret information isn't compromised, for example, by downloading. It is one thing to take a laptop. It is much easier to download the information and walk out of the building.

Are there random checks of personnel? Do our former U.S. Government employees who worked for State have access—we know some of those folks go on to work for foreign governments, as do Members of Congress, but we know that U.S. State Department people, because of their knowledge, are probably very highly prized by foreign governments. Do they have access? What are the penalties for security violations?

If a person is caught, what exactly is triggered in terms of investigation and penalty? And do you believe that those penalties are sufficiently strong to deter security violations so that they don't occur?

Let me just ask a general question, because I know we only get 5 minutes. The culture of the Foreign Service, is it too lax, you know, in an attempt to be open and reach out to governments? We know that very often even their own physical security abroad is not taken as seriously as some of us would like. Does that need to be changed?

A question on the number of months. I believe it was 8 months that lapsed between the time when the visitation policy was changed again after Tom Pickering nixed it in December. I just ask our distinguished friend from the FBI—did you advise Diplomatic Security when you found that there were foreign intelligence officers with access to the State Department and what was their reaction?

I would like to yield for your answers.

Mr. BEREZNAY. As I indicated previously, the study that was done was done in 1998. It was done in conjunction with Diplomatic Security. I believe it was prompted by a report by a State Department employee of activity that came to her attention which she felt indicated she may be being looked at by an intelligence service. So that is what prompted this. It was a diligent State Department employee, reporting this activity to Diplomatic Security. It was Diplomatic Security working with us that surfaced the unescorted visitor problem.

We did share the results of that survey. It was a very limited survey, and those results were shared with Diplomatic Security. I believe—and I will defer to Secretary Carpenter as to whether or not that report prompted his review. The timing of it certainly falls, but I don't know how much impact that did have on internal State Department policies.

Mr. SMITH. Mr. Secretary Carpenter—and if you perhaps, Ambassador Roy, or Ms. Williams might want to touch on those other questions as well.

Mr. CARPENTER. Clearly, as Tim has just said, we were aware of this information. It did drive a need for immediacy on the escort policy. I think this came, quite frankly, after our initial discussions about the need for an escort policy.

I might add, although I am not sure how pertinent it is to this, a lot of the focus that we had—Diplomatic Security had during the period that was in question was overseas. We just had two embassies blown up. We were up here trying to get more money. We were definitely focused in that area; and because of that, quite frankly, we moved slower than I would have liked to have moved. This escort policy, because it was controversial, was something that had never been done.

Let me correct that. In the early 1990's there were three countries that when their diplomats came to the State Department, were escorted. The decision was made, and I don't know by whom or based on what, to discontinue the escorts. So 1992 was the last time anyone was escorted. But, again, it was only the diplomats from three particular countries. Does that answer your question?

Mr. SMITH. It does in terms of the FBI, but in terms of the penalties—and maybe Ambassador Roy might be the pertinent person to respond to that.

Mr. ROY. The penalties fall under DS. We have no ability to apply penalties.

Mr. SMITH. How about random checks and the like and the access of former U.S. Government employees? Do they have access to the building in an unfettered way or are there checks there as well?

Mr. CARPENTER. They did. We are in the process of working with the Director General's Office to discontinue that practice and that former employees need to be escorted. If you are not currently employed as a State Department employee, you need to be escorted in the building. That process should—we have been yawing back and forth for weeks now, but that should be in place very, very soon.

As far as your question on penalties, again, Diplomatic Security doesn't punish. Are the penalties severe enough to deter? It doesn't appear so, quite frankly. I would say that the number of violations issued, and I can probably provide those to you at a later time, are much too high. It would be an indicator to me that perhaps we need to raise the bar as to what those penalties for security violations are.

Now, let me also clarify, a great number of these security violations are minor in nature. Quite frankly, no security violation—I hate to classify as minor, but these are such things as leaving a safe unlocked during a time with perhaps no secure information in it. There are certain procedures that are prudent but, again, not the crime of the century.

The more serious incidences, quite frankly, I think the Department has dealt with in a very stern manner. I would suggest it will deal in a much more stern manner in the future as a result of this. This is a very, very embarrassing situation for the Department; and if the people in the Department don't understand that, they

will obviously be made to understand it if they commit a security violation.

Mr. SMITH. Excuse me, Ms. Williams. Not to belabor the point, how hard is it to download the sensitive information to disk, which obviously is a dime a dozen and can be transported out of the building with considerable ease?

Mr. ROY. Let me comment on that briefly.

On our most secure computer systems, we do not have any downloading capability. We do not even have a floppy drive on the computers.

I would like to add a generic comment, however. If there is a culture of lax security in the State Department, I have never been part of it, and it has not been part of my Foreign Service experience, in part because of what I consider to be the superb work that DS has done at all the posts where I have served to maintain a high standard of security awareness.

I served in Moscow during the height of the Cold War. I have served in high-threat posts like Beijing and in Jakarta where the physical threat was high. In Jakarta, the inspectors concluded a year ago, after inspecting my post, that security is a dominant theme at post and has become an integral part of life in Jakarta for all mission employees.

That is the culture of security awareness that I have been part of in the State Department and I think perhaps that needs to receive a little more attention.

Mr. SMITH. Ms. Williams.

Ms. WILLIAMS-BRIDGERS. Thank you, Mr. Smith.

I would like to add to the point that Ambassador Roy has just made.

What OIG has found in the course of over 200 inspections that we have done within the past 4 years is that the attention to security overseas and handling of classified information is generally quite good. That is because when you have a chief of mission who sets a tone for the mission that security is important and there is a threat that is dominant, then people will pay attention to security.

When you have Marine security guards and regional security officers that make it their business to indoctrinate, to make people aware of and to enforce security, then you have an environment where security becomes something of importance to the people.

What we have found in the Department of State in the Main State headquarters building is that the same environment does not exist. Security was overall a very low concern for most people in the Department of State.

Moving on to your question about the penalties and the type of disciplinary action, what we found in the Department of State is that discipline did not occur as it should when there were security violations. The current policy at the Department of State is that you must accumulate five violations or infractions over an 18-month period before the situation is even referred to the Director General to take disciplinary action.

When we looked at approximately 200 cases that had been referred to the Director General, we found that 20 percent of those cases, as I understand, had at least five violations over an 18-

month period. In 20 percent of those cases, no disciplinary action was taken. For an additional 40 percent of the cases, only a letter of warning was issued to the individual. Letters of warning are pulled out of staff's personnel files after a 1-year period of time.

In the other cases that OIG reviewed, we found suspensions in 6 of the 218 cases we reviewed and 10 letters of reprimand. We do not believe that that demonstrates a commitment to take very swift and certain action against those people who have committed violations of the security policy.

Mr. SMITH. At what point does the information lead to a potential of a prosecution and how is that handled? I mean, is there a referral to the Justice Department or how is that handled?

Ms. WILLIAMS-BRIDGERS. In the Office of Inspector General, and I will defer to the Assistant Secretary for how they handle cases in DS, when allegations come to our attention that indicate a violation of law or a breach of a regulation governing security matters, and if it is a part of a larger set of allegations of misconduct against an individual, then OIG will investigate. We will certainly inform Diplomatic Security about the allegation that exists concerning a breach of security.

If the allegation merely pertains to a breach of security, then we would refer the matter entirely to the Bureau of Diplomatic Security. If the allegation during the course of a preliminary inquiry indicates that there is some evidence that a law may have been violated, we will immediately inform the Federal Bureau of Investigation and the Department of Justice and coordinate with them. They then become the supervisors, in essence, of any investigation that we might undertake.

Mr. SMITH. Let me just ask one final question, Ms. Williams. Do you feel institutionally the Department is sufficiently responsive to your recommendations on security issues? Do you receive adequate support from the top levels at the Department?

Ms. WILLIAMS-BRIDGERS. Mr. Smith, thank you for asking that question.

The Office of Inspector General shares the very same goals of the Department when it comes to security. Our goal, as is the Department's, is the protection of information, protection of our people as they work overseas and here on the domestic front, and the protection of our facilities. We work hand in hand with the Department.

That is why Congress established an Office of Inspector General, to work inside the agency, to collaborate with the agency, to share with them the deficiencies as we identify them, to identify who should be held accountable for any misconduct, any abuse or mismanagement of the funds.

I am disappointed that the Department all too often responds slowly or responds not at all to the recommendations that we make. In large part I think our working relationship is very good, but when we identify vulnerabilities in our systems that breach the very goals that all of us are trying to obtain, it is disconcerting that the Department's non-compliance results in the continuation of identified security vulnerabilities.

Mr. SMITH. Do you feel it is likely that, especially now in light of this crisis, that your recommendations—and you might want to articulate some of those, dealing with not only new procedures but

also penalties for those—I mean, nothing deters better than knowing that there is a sure and swift and certain punishment if one acts in a certain way to compromise U.S. security interests. Do you think it is likely that those recommendations will be adopted?

Perhaps anyone else on the panel might want to speak as to what really is being contemplated in a top-to-bottom overhaul.

Ms. WILLIAMS-BRIDGERS. Of the key recommendations that we have made, foremost is the transfer of responsibility to the Bureau of Diplomatic Security. We consider that matter closed. The Secretary took action to first appoint Assistant Secretary Carpenter as her senior adviser for security. That was a welcome move. I think it places in very prominent view to all in the Department the importance that she places on security.

With regard to the escort policy, which we have discussed quite a bit today, we consider the implementation of an escort policy and all the variances that have been drafted over the course of the past year to be good first steps. Even though there are holes, we commend the Department for taking the action to enhance escorts.

We are still waiting for a response and some resolution to many of the other key recommendations that we have made regarding, for example, the security incident program. We are not at all comfortable at this point that the Department has moved as quickly as it should have in instituting stronger disciplinary actions to attend to security violations.

We are pleased that the Department has taken action, that DS is looking to enhance the card swiping, identification badge system that we use, to further comply with the Director of Central Intelligence Directives that require some authentication of who is actually swiping the card.

The question was raised earlier of the Secretary's suite—the access to the Secretary's suite with the cards. Even if the system had been working the day that the gentleman in the tweed coat took the sensitive intelligence information out of the suite, that system did not comply with DCIDs. The current badge system does not allow verification that the person who is actually using the card is a Department of State employee. DS is working to address this vulnerability, possibly by use of biometric systems, and we welcome that attention.

We also understand that DS will be working with INR to attend to other DCID directives involving attenuation and inspection accreditation of the temporary work spaces, but there are some other long-standing recommendations that we have made about secure, sensitive, compartmented information access that we have not yet heard any response back to, recommendations that have been outstanding for a year now.

Mr. SMITH. Thank you very much.

Chairman GILMAN. Thank you Mr. Smith.

Mr. Hastings.

Mr. HASTINGS. Thank you, Mr. Chairman. And, Mr. Chairman, thank you for holding this hearing.

The limited time has been very candid and reflective and enlightening. I appreciate very much the witnesses being here, particularly Ms. Williams-Bridgers. I read all of your prepared statement, and I think all of us on this Committee would be wise to become

adherents to following the kinds of clarity that you put forward in that particular document.

You know something, Mr. Chairman, and all the rest of us, one of the things about this great Nation of ours is our openness is a blessing and a curse; and, when put in perspective, sometimes those of us that must, because of our partisan concerns, try to make political points, it doesn't serve usefulness to take things out of context.

For example, the problems that we are hearing about here today are serious and obviously are being addressed. But my colleague who isn't here to defend himself, and I will tell him on the floor during the next five votes that I talked about him, when Congressman Rohrabacher made the comment about there being no escort policy and it happening because of the Clinton Administration and this is like a spaghetti sieve or what have you, he ignores the fact that he served in the Reagan Administration when Secretary Shultz was in office and somebody carried a gun into the State Department and shot somebody. I mean, they didn't have an escort policy then, and they didn't have an escort policy until just a little while ago. I would just like to at least put the political ball in its proper perspective.

All of us can do it and probably shouldn't, especially when we aren't going to talk about all administrations.

What we have is a problem; and what I hear, particularly from Mr. Roy, is that the problem is being addressed from top to bottom.

I guess, Mr. Roy, the key thing is—and I would urge you in order to get us policymakers off your back—when you all have finished whatever it is that you are doing, when you have responded to the Inspector General's—as rightly you should and better in a manner that you have in the past—not you but your predecessors and those who work with you—that you make that information available to us as fast as possible as to how we can get on with our criticism our oversight requires. But it is heartening at least to know that we are in a position now that we have begun to do something about it.

Also, Ms. Williams-Bridgers, as a counter thesis to your response to Mr. Smith, I read your conclusion; and you say, I am encouraged by the actions taken by Department management to correct physical—the physical and procedural security deficiencies at State. I take that as a sign that there is progress, and I would hope that that progress would continue.

I have one question; and it is directed to you, Mr. Bereznay, Chief. Is there any evidence that sensitive, compartmentalized information has been compromised or revealed to a foreign nation while under the Bureau of Intelligence and Research?

Mr. BEREZNAY. In view of the ongoing aspect of the investigation, I respectfully request to decline answering that question.

Mr. HASTINGS. All right. I just wanted to get it out there. Because I can tell you this much also, based on Mr. Roy's statement—and I am not an investigator, but I can assure you that it is just a matter of days before all of this will be put to rest, at least in terms of who did it. Now what they did with it is yet another matter, but I will guarantee you and I will bet everybody on this Com-

mittee within a month somebody will be brought to the bar for this particular activity.

Just as a matter of levity as I close, Mr. Chairman, and recognizing that we have votes coming up—Mr. Carpenter, I listened to you very carefully. I don't know you, first time I have ever seen you in my life. But, I have listened to a lot of security people in my life. I hear candor coming from you, and I want you to know I appreciate that very much, but I bet as you walk in and out of the Rayburn Building, off and on Capitol Hill, that you see things you would certainly correct.

Thank you very much.

Chairman GILMAN. Thank you, Judge Hastings, for your nonpartisan——

Mr. HASTINGS. You can always count on that, Mr. Chairman.

Chairman GILMAN. In closing, I ask Mr. Gejdenson for any closing remarks.

Mr. GEJDENSON. Thank you, Mr. Chairman.

I just ask two things. One is, I would like to see you gentlemen in a closed session, either privately—maybe we do it in H139 and invite other Members if they want to come. So we ask some questions I felt it wasn't appropriate to ask here in a public session.

The last thing I would say is there are a lot of challenges this country faces that are very tough decisions. You have the situation in Sierra Leone, whether or not we put American personnel in harm's way, what role we are going to play.

This is actually somewhat simpler. This is—we have the resources. As a country, we ought to make sure that the national security issues that we have to keep secret are kept secret. You have to come and tell us what we need to do, and we have to work together to accomplish this. Some of the things I have heard today actually still leave me somewhat nervous about where we are in the process of protecting our secrets.

Thank you.

Chairman GILMAN. Thank you, Mr. Gejdenson.

Mr. SMITH. Mr. Chairman.

Chairman GILMAN. Please be brief. I have a couple of closing remarks, and time is running. Go ahead, Mr. Smith.

Mr. SMITH. I would just like to ask a very brief question. The head of the Civil Service Union at State, Mr. Galloway, asserted at the Secretary's town meeting that low-level employees were subject to retaliation for reporting security violations on the part of their superiors. What measures are in place to assure that retaliation does not take place?

Ms. WILLIAMS-BRIDGERS. Any employee who believes that they have been retaliated against has the recourse of seeking assistance from the Office of the Special Counsel.

Generally, the Office of Inspector General only investigates allegations of retaliation if the allegant is alleging retaliation as a result of having cooperated with the Office of Inspector General during the course of an investigation, but any other instances we would refer the employee to the Office of the Special Counsel.

Chairman GILMAN. Thank you.

Thank you, Mr. Smith.

Well, today we have heard about the serious security problems at our State Department. We have discussed some of the proposed fixes to help avoid future loss of national security information and sources and methods and, in some instances, innocent lives as well. I am calling upon our State Department to become serious and effective about security and to impose more discipline and adequate punishment where the evidence clearly warrants it in cases of any security breaches by Department personnel.

One easy, effective remedy before us is to promptly end the unescorted access possibilities for foreign press and retired State Department employees who no longer have security clearances. There is no reason why they should be treated any different than other ordinary American citizens.

I would also ask that our Assistant Secretary of State for Diplomatic Security promptly come up with a plan to end the current practice and to inform the foreign media that their gentleman's agreement is over. If they are caught unescorted in the building, their privileges should be ended.

In addition, I would like to ask Secretary Carpenter to take advantage of the FBI's offer in its testimony today to identify those hostile intelligence officers posing as media so that their access could be further restricted and their visits monitored.

With regard to Secretary Carpenter's security review I would like to urge your attention to counterintelligence efforts, a basic element of security. The Department should be prepared to protect itself.

I also urge an effective use of the possible new resources that have been provided through the recent reprogramming for personnel to manage security procedures.

Those are just a few common-sense suggestions that will not cost any funds and should have been undertaken long ago, budget cuts or not; and there should be no more excuses that these simple reforms cannot and ought not be done.

I want to thank our panelists for your very frank and candid review of the problems, and we welcome any further comments you might have or constructive suggestions as we further pursue these security problems. Thank you.

The Committee stands adjourned.

[Whereupon, at 1:10 p.m., the Committee was adjourned.]

STATUS OF EMBASSY SECURITY ENHANCEMENTS—PART II

WEDNESDAY, MAY 17, 2000

HOUSE OF REPRESENTATIVES,
COMMITTEE ON INTERNATIONAL RELATIONS,
Washington, DC.

The Committee met, pursuant to notice, at 10:05 a.m. In Room 2172, Rayburn House Office Building, Hon. Benjamin A. Gilman (Chairman of the Committee) presiding.

Chairman GILMAN. Committee will come to order. Members take their seats.

Today the Committee on International Relations is holding its second hearing of recommendations of the Overseas Presence Advisory Panel. We will be reviewing the Panel's recommendations to create a new government corporation for overseas buildings which would replace the Foreign Buildings Office in the State Department with an Overseas Facilities Authority.

This new authority will be responsible for building, renovating, maintaining and managing the Federal Government's civilian overseas office and residential facilities. In their November 1999, report the Panel stressed that our overseas institutions are not equipped to operate effectively in the 21st century, and they stated that our overseas presence is crippled by insecure and decrepit facilities, by obsolete information technology, by outdated human resources practices and outmoded management and fiscal tools.

The Panel concluded that an overhaul of the large property management program requires more authority, more flexibility and increased participation by other U.S. Government agencies with a significant overseas presence.

Presently, the Foreign Buildings Office manages 12,000 properties in more than 250 locations. With the infusion of the emergency supplemental appropriations and current increases in appropriated funds for embassy security enhancements, the task for the Foreign Buildings Office has increased dramatically.

This hearing is an opportunity to discuss the proposal for a new corporation that would operate under different rules and procedures and presumably would have greater flexibility in financing and management practices. Our Committee has heard from members of the Overseas Presence Advisory Panel. We will now hear from the State Department on this proposal.

Additionally, this Committee has been closely following the progress of enhancing the security of our overseas posts, including buying land and initiating new construction. We appreciate the staff-level briefings that have been provided since the emergency

supplemental funds were provided. We look forward to hearing from the Department on the current standing of the facility enhancement plan.

Admittedly, the State Department has a tough job of quickly trying to harden the security vulnerabilities of overseas posts, while also making certain that taxpayers' dollars are going to be wisely spent. Recognizing that fact, the Overseas Presence Advisory Panel proposed recommendations to leverage the overseas building program, which we will explore today.

Foremost, there should be no compromise when it comes to protecting our embassy employees and making certain it is going to be a safe physical environment for them. Our Overseas Presence Advisory Panel accurately captures the security situation at the State Department by emphasizing an integrated approach to security and developing a culture of security.

Establishing this security mindset, as they call it, I think will make the job before you, as the executors of the physical security program, infinitely easier.

So we want to welcome our panelists, but before we do that let me call on our Ranking Minority Member, the gentleman from Connecticut, Mr. Gejdenson, for any opening remarks.

Mr. GEJDENSON. Thank you, Mr. Chairman. Just a couple of quick things.

I think one is that we all agree that any commander——in-chief that placed military in the field without adequate weaponry, protection or intelligence, we would be outraged. If you go to some of our embassies around the world, essentially we have done the same thing, the commander- in-chief and the Congress of the United States placing American personnel, often military personnel in those facilities as well, but nonmilitary people, we have put them in dangerous situations with inadequate facilities, inadequate security. So we have got to fulfill our responsibilities if we want them to do the job overseas.

The only thing I would like to kind of throw out there at the beginning of this is the possibility that we need to review what we do in the field and whether it needs to be done there anymore.

You know, we all grow up with kind of a formative stage, and in those years you kind of decide where everything belongs. But the world has changed an awful lot, and I really question when I look at a lot of these embassies whether we need the back office overseas at all. Maybe we need to do it overseas, but maybe we need to do it like a lot of businesses, centralized, one in Asia, one in Africa, one in Europe, not that every embassy and every consulate have a very large back office that does everything, payment, disbursements and other needs of an embassy, that it may make more sense today with modern telecommunications, computer systems, teleconferencing, e-mail, that we can get a lot of what we now do in each of our embassies, where it may be difficult, we may be able to do it someplace else.

Now one of the considerations may be, if you move it back to the United States, it may be a lot more expensive. As we are all fighting over budgets, as Americans, we want to hire American nationals where we can. We don't want to eat up our whole budget in the process. Obviously, it is a lot less expensive to have the back office

in Africa or in China or in India than it is to have it in Washington, DC.

But it seems to me we have got to make some basic decisions. You may want to have regional back offices. You may want to do it in the country where there is the least threat and the most capability. You may want to take Africa and Asia and put it all in India. It is a country that speaks English. You may be able to do the same thing for Europe someplace, in Ireland or England or Scotland, so that we concentrate, we take out the back office from some of the more dangerous areas, and, you know, we are able to save money at the same time.

I look forward to hearing from our witnesses.

Chairman GILMAN. Thank you, Mr. Gejdenson.

If there are no other Members seeking recognition, we will now welcome our panelists who are here to discuss the overseas building program and related security matters this morning.

First, I introduce Mr. Patrick Kennedy, Assistant Secretary for Administration at State. Mr. Kennedy has been with the Foreign Service for 27 years, probably holds the record for the longest service as an assistant secretary for the Administration. He deserves a tribute for his outstanding service to the Department and to this Committee.

We again welcome Mr. David Carpenter, Assistant Secretary for Diplomatic Security, who appeared in our hearing on State Department security just last week. Mr. Carpenter assumed the position of Assistant Secretary in August 1998 following a 26-year career in the Secret Service. He is the first person to hold this post who has a professional background in the protection and security fields. He assumed this responsibility at a very critical time for all elements of security.

We are happy once again to hear from the Inspector General for the Department of State and Arms Control and Disarmament Agency, Jacquelyn Williams-Bridgers. Ms. Williams-Bridgers was sworn in as Inspector General in 1995. She has been with this Committee many times, and we appreciate the valuable work of her good offices.

Chairman GILMAN. So whoever would like to start—Mr. Kennedy, would you like to start off? You may summarize your statement. Your full statement will be made part of the record. Please proceed.

STATEMENT OF THE HONORABLE PATRICK F. KENNEDY, ASSISTANT SECRETARY, BUREAU OF ADMINISTRATION, U.S. DEPARTMENT OF STATE

Mr. KENNEDY. Thank you very much, Mr. Chairman. I will submit my statement for the record; and, in fact, with your permission, I will cover the highlights.

It is always a pleasure to appear before this Committee, and it gives me a particular pleasure today to update you on the many accomplishments the Department has made in improving our overseas security posture, facilities infrastructure and our worldwide facilities operations.

Obviously, since the tragic bombings of our embassies in East Africa, the issues concerning our infrastructure and security of our

missions overseas have received great attention within the Administration and the Congress. We very much appreciate the support of the Congress and particularly of this Committee for the Emergency Security Supplemental and the Administration's proposals for physical security upgrades at our overseas posts.

I would also like to say a few words today on the Overseas Presence Advisory Panel and its recommendations concerning our Office of Foreign Buildings Operations.

As you know, the Overseas Presence Advisory Panel, which issued its report last November, described many of our facilities abroad as unacceptable in terms of security and condition. Fully 85 percent of our facilities do not meet optimum security standards. Some are in need of extensive renovations. Some are seriously overcrowded. Most, however, simply have to be replaced.

To protect our employees overseas, our goal is to expeditiously relocate into safe facilities more than 22,000 embassy staff in over 220 vulnerable buildings. This is a formidable task. Achievement of this task will require an enormous initial and sustained level of capital investment.

Mr. Chairman, quite frankly, during the past 10 years we have neither requested nor received sufficient funding to allow us to maintain our infrastructure base. Most recently, since the 1998 bombings, we are finally beginning to arrest that decline in resources, thanks to the support of the President and the Congress, and have taken the first steps toward rebuilding our facilities infrastructure.

In fiscal year 1999 alone, the Office of Foreign Buildings obligated over $800 million, the most ever obligated in a fiscal year, to replace unsafe facilities and improve our security at those posts where facilities cannot be replaced for several years.

As part of the Overseas Presence Advisory Panel's overall charter to evaluate the way the United States organizes its overseas activities, it made 44 recommendations. This morning I would like to focus some of my remarks on the Panel's recommendation to establish an Overseas Facilities Authority, as yourself have noted.

The Panel advocated replacing the Bureau of Administration's Office of Foreign Buildings with a federally chartered corporation, an Overseas Facilities Authority. The issues that led to the Panel's proposal included the perception that A/FBO-managed construction projects took longer and cost more than comparable private sector projects, the timelines were not always met and that staffing levels appeared to be too high. However, I believe that the staff work that underpins these perceptions is faulty, as it fails to give due consideration to security requirements and special overseas needs.

The Panel proposed creating a government-financed corporation. This new authority would exercise responsibility for building, renovation, maintaining our overseas civilian facilities. The Overseas Facilities Authority, in addition to receiving annual appropriations, would have features not currently available to us in the Department now, including receiving funds from other agencies, levying capital charges, obtaining forward funding and loans from the Federal Treasury.

The Overseas Facilities Authority, again unlike the current FBO, would have the ability to apply management techniques commonly

used in the private sector to include financial incentives and performance-based compensation standards. The Panel reasoned that higher salaries and incentives would allow OFA to attract highly qualified real estate and other professionals and further motivate employees.

We are currently giving serious and careful consideration to the Panel's proposal. An Interagency group headed by the Director of the Office of Foreign Buildings Operations, Patsy Thomasson, is reviewing all aspects. Earlier this year, Ms. Thomasson formed six teams to look in and analyze in depth five critical areas: organizational structure, financing, business process reengineering, customer focus and communications. A sixth team manages the overall effort. Together, these teams will make recommendations on how the Panel's desired outcomes, which we all agree with, can best be achieved. We have also contracted with a leading consulting firm to examine various options and ways to make FBO a more performance-based organization.

While these efforts are continuing, I believe that creating an independent OFA is not essential to accomplish the changes that OPAP laid out and which we agree with. Most of the proposed attributes of the Overseas Facilities Authority could be assigned either administratively or legislatively to A/FBO without disrupting or halting the very positive direction in which A/FBO is now headed.

Although we agree with the thrust of the Panel's recommendations, we question whether the creation of an independently Federal chartered organization is necessarily the best approach to meet our infrastructure challenges. Principally, we are concerned that such an entity may compromise the vital link between foreign policy and facility decisions. For example, there are foreign policy issues such as reciprocity that are intricately intertwined with overseas facilities programs, such as the case with China where we are seeking a new site for our embassy in Beijing, and China is seeking as a condition a site in Washington. Such is also the case with the United Arab Emirates, where we are seeking to acquire a parcel of land, and they wish to procure land in Washington. These are classic examples where facility decisions are affected and sometimes driven by foreign policy considerations.

The Panel also urged that we continue to implement the Accountability Review Board—the Crowe Commission proposals. We are doing that, and I am pleased to report that Foreign Buildings has been particularly successful in responding to the mandates of the security supplemental. Interim facilities are fully operational in Dar es Salaam and Nairobi, and we are moving smartly toward constructing permanent facilities in both locations.

Foreign Buildings Operations conducted a competition for its fast track design/build contract and awarded this contract last September. The designs of these projects have now reached the point where we anticipate giving the contract the green light to mobilize onsite in Dar and Nairobi next month. We also opened temporary buildings in Doha and are fitting out three buildings in Pristina to serve as temporary facilities, and we have permanent construction already under way in Doha and Kampala.

Currently, we have 14 new embassies of consulates in various stages of development. We are also in the process of acquiring several additional new office building sites, and since the bombing FBO has completed 15 major rehabilitation projects at overseas posts with another 46 major rehabilitation projects ongoing at this time.

We have also relocated many Department and other agency personnel to more secure facilities. For example, AID personnel have been relocated to more secure facilities in some dozen locations around the world.

Increasing setback from streets and other buildings is another way of reducing this threat. During the past year and a half, FBO has been extremely active in acquiring 87 properties in 25 posts around the world to provide greater security. Negotiations and investigations are continuing for another 31 properties at 14 posts.

Worldwide security upgrade funding was appropriated and has enabled us to approve over 1,000 security upgrade projects at overseas posts, and 34 have already been completed. Every project will further protect our employees. This program includes projects such as the installation of berms and bollards and access controls, is being executed by FBO, the post itself or by American companies under implementation or basic ordering agreements.

Other components include the installation of shatter-resistant window film and the installation of ballistic-resistant doors and windows. The bombings in Africa tragically demonstrated the greatest threat to life and injury from a bomb is flying glass shards. Since the bombings, we have purchased 5.5 million square feet of window film. Nearly half has been installed, and the remainder is in the process of installation. We have also installed or replaced over 500 security doors.

The FBO's Asset Management Program, which essentially acquires properties by using proceeds of sale from excess or underutilized properties, has been very successful, purchasing 18 properties last fiscal year, and in the first half of this fiscal year has already disposed of 17 other properties.

These successes are the result of retorquing internal processes, applying new initiatives and introducing innovative methodologies. These have been the key factors in achieving FBO's high level of productivity. Today's Office of Foreign Buildings is not the same as in the late 1980's and early 1990's under the Inman program.

A 1991 GAO review of the management of the Security Construction Program revealed problems that FBO experienced during its efforts to meet the challenges of the Inman buildup a decade ago. The most significant difficulties relate to inadequate staffing, difficulties with overseas site acquisition, contractor performance and the lack of an extensive strategic focus. Since those years, however, FBO has implemented lessons learned throughout the organization and is now well prepared to undertake a large construction program.

FBO has developed an improved strategy for effectively executing a difficult, expanded construction program and has augmented its staff to handle the workload. This strategy is derived from FBO's Inman experience with the simultaneous execution of large, multiyear projects and for implementing private sector construction

industry best practices. These include design/build contracting where you can cut time and effort off the project by working with the private sector.

We are looking into other multiple projects that could be packaged into groups for an award to a single large design build American contractor as we have successfully done in Dar es Salaam and Nairobi. Additional design build projects could be awarded for groups of projects in the outyears. These efforts are managed by an integrated project management team that provides effective controls and added expertise.

In the staffing area, FBO is much better positioned than in the mid 1980's when the Inman program began and its in-house work force numbered less than 200. The professionalism and depth of the work force has increased as its size has grown to over 760 today. Eighty-four new staff members have been or are being brought on board for the worldwide security upgrades alone. Additional real estate professionals have been hired to find and acquire new buildings and sites, and more design, engineering, project management and other professionals and specialists have been brought on to execute construction projects.

Contract support has been increased, furthermore, by teaming with two American companies, the Perini Corporation and Brown and Root to assist in security upgrade work and with other indefinite quantity contractors that increase FBO's capabilities, especially in design review.

The Accountability Review Board discussed our priority setting, and they recommended spending $14 billion on embassy construction in the next 10 years. Interagency Embassy Security Assessment Teams determined that most of our posts have compelling facilities needs such as inadequate setback, structural hardening, relocations and other security requirements.

All chanceries, consulates and multi-tenant buildings have been evaluated. The analysis assessed the soundness of each building's structure and facade, the adequacy of the perimeter security, the setback from adjacent properties, the political violence threat, and additional security consideration that included the capability and willingness of the host country to control its internal and border security. The resulting ranking was reviewed by stakeholders—regional bureaus, other government agencies, Diplomatic Security, the ESA teams and FBO. They were also reviewed and concurred in by the Under Secretaries for Political Affairs and Management. These projects are then planned for different fiscal years based on vulnerability, stakeholder input and consideration of other factors.

Other measures developed or enhanced since the 1998 bombings. Time and space preclude me from a full explanation of all these factors which I will submit for the record, but these best practices, in their aggregate, add to the intense efforts by the Department which have resulted in an outstanding record of achievement over the past 18 months and clearly demonstrate that today's FBO has the ability to manage a large and complex building program.

Mr. Chairman, we believe that the efforts that we have undertaken with your assistance over the past 18 months have led to a new paradigm, and we are prepared and able to take the funding that you have been so helpful in providing to us to expand security

of our employees and the employees of all U.S. Government agencies overseas.

I now turn to my colleague, Mr. Carpenter.

[The prepared statement of Mr. Kennedy appears in the appendix.]

Mr. MANZULLO [presiding]. Mr. Secretary, we appreciate your comments; and, as you know, Congress did not flinch at making the funds available in order to provide for security.

Our next witness is Assistant Secretary David Carpenter with the Bureau of Diplomatic Security at the Department of State.

Mr. Carpenter, if you could summarize your statements and keep your talk to around 10 minutes or so, as did Mr. Kennedy, we would appreciate it.

Mr. CARPENTER. Yes, sir, I will.

STATEMENT OF THE HONORABLE DAVID G. CARPENTER, ASSISTANT SECRETARY, BUREAU OF DIPLOMATIC SECURITY, U.S. DEPARTMENT OF STATE

Mr. CARPENTER. Good morning, Mr. Chairman and Members of the Committee. I welcome this opportunity to testify before you on the security profile of our facilities overseas.

On August 7, 1998, our embassies in Dar es Salaam, Tanzania, and Nairobi, Kenya, were bombed simultaneously by extremists bent on the destruction of American presence throughout the world. These tragedies unleashed a massive and intense effort to provide much-needed security improvements at all of our overseas posts. Although much has been accomplished, more needs to be done. Our overseas facilities are generally more secure now than in August 1998, but the continuing threat environment worldwide requires that we not lose focus, that we continue to explore new ways of protecting ourselves and support a program for new embassy construction.

The Department has aggressively upgraded security at previously low and medium threat posts to standards that were formerly only applied at high or critical level embassies or consulates. High and critical level posts also received significant upgrades of equipment to better fortify their facilities. We no longer believe, in an era of transnational terrorism, that we have low or medium threat posts, nor do we believe that we will receive tactical intelligence of an imminent attack. Simply put, we must be prepared for any eventuality that presents itself.

Our goal following the bombings was to immediately improve the security of our threatened consulates and embassies, and we have done so. But at the outset let me say that it is important for this Committee to know that we still have a very basic problem that cannot be fixed quickly. The vast majority of our diplomatic posts fail to meet one of the most basic security standards, namely, the hundred foot setback standard. Until we can build embassies meeting the setback and other security standards, our efforts cannot provide the degree of security all of us want for our people and facilities.

Having recognized that we still have grave security concerns overseas, it is also important for the Committee to know that we have done a lot and that our embassies and consulates are more

secure now than ever before. In this regard, let me review for you what we have done through our security upgrade program. Some of these actions have been based solely on DS initiatives; others were suggested by the Accountability Review Board chaired by Retired Admiral William Crowe, the report of the Overseas Presence Advisory Panel and the Office of the Inspector General.

As previously stated, we are aggressively upgrading security at low and medium threat level posts to standards that previously only applied to high and critical rated posts. We have put in place physical security upgrades at our embassies and consulates such as reinforced perimeter walls, bollards, new guard booths, vehicle barriers and shatter- resistant window film. We are upgrading and deploying security equipment to include better lighting, cameras, video recorders, bomb detection equipment, armored vehicles, alarm and public address systems and X-ray equipment. Where possible, we have mitigated the lack of sufficient setback by closing streets and provided for mandatory vehicle inspections.

We have also expanded our antiterrorism assistance training to aid foreign police in combating terrorism through appropriate programs as surveillance detection, border security, explosive detection, crisis management and maritime security.

In addition, we have installed alarm systems at embassies and consulates to alert personnel to impending emergency situations and have instituted a program for the employees to duck and cover when the alarms are sounded.

We have also created a new security environment threat list with a modified methodology and criteria for determining threat levels. This process now addresses transnational terrorism as a distinct category as well as the threats from indigenous terrorism and political violence and the threats from intelligence services, both technical and human, and, of course, crime.

DS has also changed the focus in training courses for regional security officers and special agents to give them greater training on counterterrorism methodology, explosive ordinance recognition and disposal, chemical/biological weapons threats and defenses, and surveillance detection techniques.

In response to a specific recommendation from the Accountability Review Board, we are also working with the FBI to better analyze law enforcement information which might have a bearing on threats to our missions overseas and to more quickly disseminate that information to appropriate posts. To that end, a DS special agent has been detailed to the International Terrorism Section at FBI headquarters, and DS special agents are participating in the FBI's Terrorism Task Forces around the country.

DS has also established the office of The Coordinator for Chemical Biological Countermeasures. That office, which is conducting a worldwide survey to determine vulnerabilities, has purchased and is distributing chemical biological equipment to all posts. As part of its educational program, it has distributed instructional materials, including pamphlets, videos and a series of cables, to alert all posts to the nature of the threat and to provide defensive guidance. It has also established a comprehensive training program for security professionals and first responders.

The newest addition to our program and of major significance has been the establishment in less than 1 year of a surveillance detection program at almost all of our overseas posts. A critical lesson learned from the bombings in East Africa is that there is an intense surveillance conducted against our facilities prior to an attack. Since going operational in January 1999, surveillance detection teams, most of which work with host government security services, have observed over 700 suspected incidents of surveillance against our personnel and facilities worldwide. It has in a sense expanded our security perimeter and zone of control beyond our previous limitations. The surveillance detection program is clearly a work in progress, but we feel that it is destined to become a major aspect of our overseas security defenses.

Finally, and I believe most importantly, DS has hired 234 new special agents and 17 security engineering specialists, which has allowed for the creation of 140 new security officer positions overseas. By the end of fiscal Year 2000, we will have 420 DS special agents serving as security officers in 157 countries. DS has also hired 20 additional diplomatic couriers, 34 maintenance technicians and 46 civil servants in support of overseas security.

Mr. Chairman, as you know, this is National Police Week. On Monday on the very grounds of this Capitol we paid tribute to this country's law enforcement heroes who gave their lives in the line of duty in the past year. Over the years, Diplomatic Security has had its own heroes, some who gave their lives and others who have lived to continue the fight. I am positive out of this new cadre of special agents and other security specialists we will have more heroes.

I thank this Committee for its support in hiring these new people and hope that I can look to you for support as we seek additional positions to strengthen our programs. It is people that will make the difference, that is, trained, motivated and dedicated professionals with the single purpose of ensuring the safety of our overseas personnel and facilities.

Mr. Chairman, with regard to your request for my views regarding the creation of a new agency to replace FBO, let me assure you that we have enjoyed a positive and close working relation with FBO as is necessary to support our diplomatic personnel, to improve security and to upgrade our facilities worldwide. We have a construction security management group working within FBO that helps to strengthen this partnership. I do not believe that distancing DS from FBO would enhance our security effort. Furthermore, I personally do not see how an independent entity would be more capable of overcoming the challenges and obstacles that FBO currently faces.

You have also asked for my views on the OPAP proposal to make greater use of regionalization as a means to reduce the number of personnel needed at posts and for my views on whether any posts would be downsized or closed because of security threats.

OPAP recommended creating a process to right-size our overseas presence, reduce the size of some posts, close others, reallocate staff and resources and establish new posts where needed. State and other agencies formed an interagency committee to review how to implement the right-sizing recommendation in the OPAP report.

In early March, a pilot program began at a number of posts for the purpose of developing recommendations for right-sizing at these posts and to develop criteria that can be applied universally. What I have seen thus far, Mr. Chairman, suggests that regionalization efforts could result in reducing the size of some posts but would inevitably result in increasing the size of others. But from a security standpoint, I doubt that there would be any measurable savings in such an effort.

My concerns are primarily focused on decisions related to where the regional posts are to be located and assurances that the prescribed security standards are in place. Certain countries present particularly difficult environments in which to work. By that I mean high crime, inadequate infrastructure, unstable governments, poor police support and so on. Yet they may provide a geographical advantage as they are centrally located as hubs for air transportation or viewed as gateway to a continent. Believing that security is an important factor when entertaining ideas of regionalization, it is critical that no decision be made without proper vetting of life safety issues related to these regionalization issues.

Mr. Chairman, this concludes my testimony. As I indicated at the beginning, we have been diligent in our efforts to upgrade security at our overseas posts, and we have been successful in making those facilities safer now than ever before. Nevertheless, there is still much that needs to be done, and until all of our facilities meet the basic security requirements none of us will be satisfied with our security posture overseas.

I appreciate your interest and the Committee's interest you have taken in this topic and will be happy to answer any questions when appropriate.

[The prepared statement of Mr. Carpenter appears in the appendix.]

Chairman GILMAN [presiding]. Thank you, Mr. Carpenter.

We will now proceed with testimony by Ms. Williams-Bridgers, and you may summarize your testimony, and we will make the full statement a part of the record.

STATEMENT OF THE HONORABLE JACQUELYN L. WILLIAMS-BRIDGERS, INSPECTOR GENERAL, U.S. DEPARTMENT OF STATE

Ms. WILLIAMS-BRIDGERS. Thank you, Mr. Chairman, Members of the Committee. I appreciate the opportunity once again to testify before this Committee on the Department of State's efforts to manage the embassy security enhancement program. As demonstrated by the terrorist attacks on U.S. embassies in Nairobi and Dar es Salaam in 1998, perhaps no greater challenge exists for the Department than providing adequate security to protect our people, facilities and information.

As you requested in your invitation to this hearing, Mr. Chairman, I will review the work done by the Office of Inspector General on the Department's management of the embassy security enhancement program, its use of the Emergency Supplemental Appropriations and its compliance with overseas security standards.

Since the bombings of the embassies in Nairobi and Dar es Salaam security oversight has become an even more critical mission

for the Office of Inspector General. We now have multidisciplinary teams in OIG to evaluate the implementation of physical security initiatives and to monitor the expenditure of the $1.5 billion emergency supplemental.

In the 18 months immediately following the August bombings, OIG evaluated the physical security and emergency preparedness of 42 embassies.

The most significant security challenge for the Department is the protection of overseas employees lives while at work and at their residences. From a physical security standpoint, this means upgrading the perimeter security of buildings, especially chanceries; building new chanceries to replace those that are clearly unsafe; and collocating U.S. Government agencies overseas into protected areas. Another significant challenge is the protection of classified material, which is increasingly becoming electronic information, both on the domestic front and overseas.

It is evident from our examinations of the various elements of embassy protection that setback is the preeminent security concern for our overseas posts. Setback provides the greatest protection from vehicle bombs. The OIG has made recommendations that could effectively increase setback, some at relatively low cost. For example, we have recommended that embassy officials work with the local government to alter traffic patterns around the mission, and in other locations we proposed creating increased setback by extending control over street parking spaces. However, at other missions the only way to effectively increase setback is to purchase adjoining properties, and at other missions we must move to a new location to achieve a meaningful setback. Both options could cost millions of dollars. To meet setback requirements and other security standards, 34 of the 42 embassies we inspected within the last year would require new chanceries and compounds. However, only five of the posts have a new chancery under construction or planned in the next 5 years.

The ideal embassy would be protected by at least 100 feet of setback. It would be constructed to current security standards and have a well-lit, well-constructed perimeter wall; and it would be under constant surveillance by closed circuit television. Beyond the wall, a surveillance detection unit would determine whether possible terrorists were surveilling the mission. A local guard force would protect the perimeter. Entrance to the mission compound would be well controlled. The chancery would incorporate a number of physical security measures to protect against bomb blasts and offer safe haven if the compound was breached.

Overseas Security Policy Board standards provided the framework for our security oversight inspections. Let me emphasize that none of the 42 embassies the OIG inspected met all security standards. Incremental security improvements such as upgraded walls, doors and windows cannot fully compensate for the lack of sufficient setback. In addition, over 50 percent of the posts we inspected did not meet standards for window protection, perimeter wall, vehicle inspection areas, chancery wall and door construction or exterior lighting and closed circuit television.

At about one-third of all locations we reviewed, we recommended measures to upgrade security barriers, exterior lighting and anti-

climb fences. We recommended the installation of vehicle barriers at entry gates. We recommended revised local guard vehicle access control procedures and the upgrade of public access control. In addition, we reviewed local guard services and recommended program improvements or greater post management supervision at about one-third of all locations.

Further, to mitigate the effects of flying glass resulting from a car bomb attack, the Department is replacing old and often defective 4-mil shatter-resistant window film with a higher standard of protection. While the Department concurs with the Accountability Review Board that ballistic laminated windows provide superior protection against a car bomb attack, the majority of our overseas facilities cannot structurally support this upgrade. A more practical solution is to purchase and install 8-mil shatter-resistant film on all windows. The Department plans to do this by July 1, 2000.

Our review of the interim office buildings for our embassies in Dar es Salaam and Nairobi addressed the management challenges to provide secure facilities and better protect employees of the Agency for International Development [USAID]. Foremost among our concerns for the interim office buildings is the lack of collocation and the imminent need for the Department to address the security concerns for those agencies that are not located on the interim compound. Similar collocation concerns have been raised for the new embassy compounds in Luanda and Kampala.

In addition to the physical security initiatives, the Department has implemented a number of initiatives that will enhance an embassy's ability to handle a crisis situation, including emergency alarms and drills, expanded emergency planning programs, and emergency communications. In many cases, management-supported procedural initiatives can improve embassy security without any expenditure of funds. As an example, during our inspection of the temporary embassy compound in Doha, Qatar in August 1999, we cited the need for a post to establish a proactive working relation with the host government's protective service to ensure a cooperative and timely response to a terrorist threat.

The Department has also initiated a worldwide surveillance detection program to detect and deter potential terrorist attack. As Assistant Secretary Carpenter suggested, it is a work in progress. But it is a commendable effort. Preliminary results of our review indicate a need for the Department to improve reporting criteria for regional security officers and to make better use of information collected during surveillance.

Some of the most difficult security issues to correct both domestically and overseas deal with information security. OIG has completed over 20 audits identifying vulnerabilities in information resources and security management. In many ways, improving information security may be a bigger challenge than improving physical security because of the many fixes that involve a change in employee behavior rather than the procurement of additional technical equipment.

In my statement before this Committee last week I discussed the specific deficiencies that have perpetuated a lax security environment in the Department of State. Therefore, I will not belabor the

point today regarding the need to pay better attention to security on the domestic front.

Overseas, there are many reasons for the vulnerable condition of American posts. Lack of funding obviously plays a role. The Accountability Review Board estimated that $14 billion would be needed over the next 10 years. However, as Mr. Gejdenson suggested in his opening remarks, the size of our presence overseas must also be considered as we examine how to best protect U.S. Government officials who reside and work abroad. The right answer to "right-sizing" lies in providing the staffing, the financial support and security required to do the job that needs to be done. Regionalization may sometimes make sense because of the economies, efficiencies and safety of operations that may result. However, regionalizing operations does not always make sense from a security perspective. Such concentrations sometimes create larger, more inviting targets for terrorism. Embassy Nairobi, for example, hosted several regional offices.

Looking ahead. Mr. Chairman, in your invitation to testify this morning you asked that I address the ability of the Department to manage a security enhancement program and the status of various initiatives. I focused my remarks on how the Department has responded over the last 18 months in its management of emergency security initiatives. The tragedies in Africa have captured the attention of the Department, of this Congress and the American public. Meanwhile, recent security lapses at home have been a wake-up call that other aspects of security just as vital to the defense of American interests as physical security also need attention.

The Department has responded well to the need to move quickly in the aftermath of the bombings and to use emergency funding provided by Congress. The Department's continued success is dependent on how well and how long it exercises disciplined attention to effective security practices and how long the U.S. Government and the Congress remain committed to funding the construction, maintenance and continual improvement of that infrastructure.

As we embark on this expensive commitment, the requirement for the Office of Inspector General to provide specialized oversight of the use of funds also increases. As the Department moves from the emergency response to a longer term, more strategic approach for the rebuilding of our foreign affairs infrastructure, so must the OIG move forward with monitoring these initiatives.

With the exception of a small one-time emergency supplemental appropriation in fiscal year 1999, funding for OIG has been straightlined since fiscal year 1996. Increased funding for security and for those charged with overseeing security improvements for you and the Department is only one of the ingredients necessary for rebuilding infrastructure and changing attitudes toward security, but it is a vital ingredient for all of us. As always, Mr. Chairman, the continued support of this Committee for OIG in this regard is much appreciated.

That concludes my summary. I will be glad to answer any questions you have.

[The prepared statement of Ms. Williams-Bridgers appears in the appendix.]

Chairman GILMAN. Thank you to all of our panelists for your good testimony. We will now proceed with questions.

Mr. Kennedy, the General Accounting Office reported on the Emergency Security Supplemental program in March pointing out that, as of December 31, 1999, the FBO obligated $360 million out of some $627 million, and actual expenditures were $83.6 million. Have those figures changed much since December?

Mr. KENNEDY. Yes, Mr. Chairman. As of now, if you take the funding that was made available and you combine, since this is a moving target, the funding that was made available in both fiscal year 1999 and fiscal year 2000, we have already obligated and committed almost 70 percent of the total funds that have been made available to us.

Chairman GILMAN. Of the 70 percent, how much of that has actually been spent?

Mr. KENNEDY. Actual obligations are—of the $627 million, we have obligated $379 million, and we have committed $62 million. Under the arcane system that the Federal Government uses, when I issue a purchase order or a contract to a vendor, I am committing that money in full. I then only pay that contractor for the work that is in progress. But the obligation rate is the rate that governs exactly how many projects I have under way, Mr. Chairman.

Chairman GILMAN. We have only spent some $60 million?

Mr. KENNEDY. No, Mr. Chairman. We have obligated three hundred——

Chairman GILMAN. I know what you obligated. I want to know how much you have actually spent.

Mr. KENNEDY. I will have to get the liquidation——

Chairman GILMAN. Well, roughly what have you spent? What have you spent so far? Forget the obligation. What has actually been paid out?

Mr. KENNEDY. I will have to get that for the record.

Chairman GILMAN. Can you give me an estimate?

Mr. KENNEDY. I would say that we have probably liquidated on the order of half of that amount.

Chairman GILMAN. Half of what amount?

Mr. KENNEDY. Half of the $379 million that we have obligated.

Chairman GILMAN. So you have spent about $150 million to date, actually laid out?

Mr. KENNEDY. Cash out of the till, yes, sir, versus obligations, yes, sir.

Mr. GEJDENSON. Would the Chairman yield for one moment?

Chairman GILMAN. Yes.

Mr. GEJDENSON. Just so I understand this, so what you are saying is if you were to buy a new wall in front of an embassy and that wall was to cost $5 million, that means you can't spend that $5 million again even though you haven't actually handed it to anybody. So now you have this $5 million that is obligated but not spent. Then as the contractor finishes one-fifth of the wall, if you were a prudent manager you would give him slightly less than one-fifth of the money, is that correct?

So the process is what you would normally have in any construction project. If you build a house and you go to the bank and you borrow $200,000, you don't walk over and spend, Mr. Chairman,

$200,000 to the builder. You say, here's $200,000 and say I hope I have a house at the end. What you do is you obligate $200,000—it is a very inexpensive house because I am a democrat—and then when he finishes—you might give him some of it to begin with, and when he finishes, say, half of it, you might give him $80,000.

Chairman GILMAN. If the gentleman would yield, I realize these basic concepts, but what I am asking about——

Mr. GEJDENSON. It doesn't allow them to——

Chairman GILMAN. If the gentleman will yield.

Mr. GEJDENSON. It is your time.

Chairman GILMAN. Thank you. We approved all of this in October 1998. Here it is over 2 years later, 2½ years later, and we still have only spent about $150 million out of the $1.5 billion.

Mr. KENNEDY. Mr. Chairman, if I might add, for example, we have executed large contracts for the constructions of the embassies in Nairobi and Dar es Salaam. Those are significant expenditures. Specifically, we asked for those moneys to build the new embassies in Nairobi and Dar es Salaam, and you graciously assisted us in getting those.

Chairman GILMAN. But—if I can interrupt you, Mr. Kennedy—but the fact is your obligation is only $600 million. Where is the rest of the money and why are we so slow in committing these funds?

Mr. KENNEDY. Mr. Chairman, if you take the emergency appropriation, the money available to FBO for its part of the activity was $627 million. Other parts of it were to pay the Defense Department for services that were provided to us during and after the crisis, were for medical expenses and other people injured in the crisis, were for payments, almost ex gratia payments to the governments of Kenya and Tanzania for damage done in those cities, funding as Mr. Carpenter has outlined for all the new security agents that he has brought into place. So the total package of $1.5 or so billion, the amount of money that was given to me to expend on bricks and mortar was $627 million, and so I am playing with $627 million on the books, and that is what I have been working through, Mr. Chairman.

Chairman GILMAN. Is that fully obligated, the $627 million?

Mr. KENNEDY. No, Mr. Chairman. Of the $627 million we have obligated $379 million.

Chairman GILMAN. All right. So, again, Mr. Kennedy, I am asking you, you have had this since 1998. You have only obligated half of it. Why has there been a delay in the rest of the funding?

Mr. KENNEDY. Because, Mr. Chairman, when we worked through this effort, it is divided essentially into the bricks and mortar side, which has three parts. The first part is buying adjacent properties. Because we have learned, as both Mr. Carpenter and the Inspector General has pointed out, one of the best things we can do is expand the setback, the distance between our building and the nearest point the terrorists can reach. So over this period of time we have acquired 87 properties. We know that one of the major things we need to do is buy more property. So in 31 other locations, we are negotiating with the landlords right at this moment. So I have to set aside money in order to complete those.

The properties—in many cases, the landlord has let us put our barriers around them, so we have achieved the setback already, but the cash has not moved out of my hands on behalf of the U.S. Government to the landlord until title searches are complete. So I have achieved the security purpose, but I will only spend the money when he gives or she gives me clean title. That is an example in that regard.

Chairman GILMAN. So it's a balance of the unobligated funds virtually committed to your land purchases?

Mr. KENNEDY. No, sir, part of it.

Chairman GILMAN. How much of it is for land purchases?

Mr. KENNEDY. A total of $41 million was set aside for land purchases. We have spent 27 out of the 41. So there is still $14 million. So I have spent about two-thirds of it on land purchases, and the other third is pending on the process of negotiating with landlords in order to——

Chairman GILMAN. That is beyond money you are going to obligate for land purchases. What is the plan for the remainder of the money?

Mr. KENNEDY. For example, the total price to stand up Nairobi and Dar es Salaam is about $163 million. That is for those two buildings there. We have obligated $115 million. There is another $94 million yet to obligate. Why is that, Mr. Chairman? Because we also furnish the building. We provide furniture, we provide generators, we provide telephone systems for those buildings. We only buy that equipment at the point in time because I wouldn't want to buy a telephone——

Chairman GILMAN. In addition to the equipment and land purchases, money remaining for completing construction, where is the rest of the money?

Mr. KENNEDY. Then there is the worldwide security upgrade which is the berms, the bollards, the new perimeter walls, the new security access points. Of the $212 million in that program level, we have obligated or committed $159 million of that. They have done the architectural engineering work; and they have now, for example, submitted the bids which we are evaluating so they can build these major additions.

Mr. GEJDENSON. Would the Chairman yield?

Chairman GILMAN. Yes.

Mr. GEJDENSON. Thank you. So let me ask you, your total is $627 million that you got to look at to spend for security.

Mr. KENNEDY. For bricks and mortar.

Mr. GEJDENSON. Bricks and mortar. How much of that do you have a plan for?

Mr. KENNEDY. We have plans for all of it.

Mr. GEJDENSON. So basically the difference between what you have been authorized to spend on bricks and mortar and what you have obligated or spent is a function of process. It takes time to get architectural drawings, and what we are talking about is you have spent 2 years trying to spend this money. I guess my question is, or my statement would be, is this Committee would cause you serious damage if you ran out and spent that money the first day without doing the title search, without getting the drawings, without getting the bids.

I think, Mr. Chairman, they are doing a pretty good job in spending money, generally Republicans aren't in a hurry to spend money, but I am glad to see we are both committed to fixing these security issues. I don't think there is an issue here. I think if you look at the normal contracting process, if it was the House of Representatives or any other institution, that this 2-year period is not an unreasonable length of time to go through the process of coming up with plans, to doing the bidding, to doing the research on title and to then executing contracts.

Chairman GILMAN. Thank you for your testimony, Mr. Gejdenson.

Mr. GEJDENSON. You are welcome, Mr. Chairman. The clock doesn't seem to be running today. I thought I would get it in before the evening news.

Ms. WILLIAMS-BRIDGERS. Mr. Chairman, may I also offer something here?

I think another reason for what appears to be a fairly low obligation and expenditure rate is that the Department did experience I believe during the first three quarters of 1999 a fairly favorable exchange rate, which meant that the amount of funds that they actually had to obligate and expend were much less than what they had anticipated.

Chairman GILMAN. So does that mean you have a surplus now? I don't think you have to respond to that.

Mr. Kennedy, before my time runs out, please update us on the implementation of these construction projects. My understanding was that 119 posts were to be surveyed for improvements, but in September surveys were suspended with 75 posts, then reviewed because of the cost of the project, and as of December 1999, only one project had been completed and seven were in a construction or design building stage. Have any more of the perimeter projects been initiated?

Mr. KENNEDY. Mr. Chairman, the security improvement is a four-part effort, and if I could take them in reverse order, the fourth part is window improvements and door improvements. In that case, 230 posts have already received their funding for the window improvements, and all the new window improvements will be completed by June of this year, and we have installed 160 new security doors.

The second part of it is projects that are under way at post. Posts have completed 272 projects at 178 posts. That includes examples like closing of streets in Abidjan and building barriers in the streets; in Cotonou, installation of barriers that push the setback to a hundred feet. In Budapest, we leased a park with the concurrence of the local government and pushed our security perimeter out, and so there are 272 projects now completed at 178 posts.

Then we move down into what we call the mega projects, the projects that no post can complete on its own because they do not have the architectural and engineering capabilities nor does the host nation often have those abilities. So, we can't safely turn them over to the posts because you certainly don't want to use firms that fall below the level of providing good security. In those cases, we do do the security projects. We turn to American contractors and have an American architectural and engineering firm go to the post

and develop the scope of work according to the standards that Mr. Carpenter's membership on the Overseas Security Policy Board provides to us.

Those are the security surveys that are being done. We've done 72. We have awarded 18 construction contracts to American corporations, and we have also done eight additional projects, five of which are in design and three are in the design/build process. So when you say there is only one completed, there is one completed out of one-fifth of all the efforts involved, the mega projects. The others are the slides I showed during my testimony, which showed that we are under way with the bulldozers, the backhoes——

Chairman GILMAN. Mr. Kennedy, let me interrupt. Do you have additional funds in your fiscal year 1999 slated for 2000 for continuing to work on these projects?

Mr. KENNEDY. Yes, sir, that is the money we have not yet spent.

Chairman GILMAN. I am going to reserve the balance of my time. Mr. Gejdenson has to attend another meeting. Mr. Gejdenson.

Mr. GEJDENSON. Thank you, Mr. Chairman.

Again, I would just like to say on this anybody who has built a home, it takes 10 months once you have got plans, approval from the zoning folks, if you have got your drawings in place. I think what we want is a good quality project. At the end, we want to get our money's worth. I am sure you are getting bids that are off the charts because they figure the U.S. Government, you have got unlimited money and so it takes some time to renegotiate these. I want you to do a good job, I want you to do a careful job, and I don't want you to waste a lot of money. So don't just rush and dump these buckets out the window so you can come become here and say, yes, we have spent all the money.

Let me ask you, Mr. Carpenter. There was a proposal to set up a new government corporation to solve all of these problems. I am a little skeptical of new corporations. I am like the 100-year-old man. They told him, I bet you have seen a lot of changes in your life. He said, and I have been against most of it. I think I am getting to that point. Because we move the chairs around, we create a whole new set of bureaucracies, I am not sure we solve any problem.

Putting aside new government corporation, of the authorities they say this corporation should have, do you not have any of those now and do you need them? You get my question? Because it is new corporation, here's the authorities the corporation have. If we got rid of the idea of a new corporation, we go to your organization and we say, all right, here are the authorities we are going to give them. Do you need any of those? Do you not have any of those now?

Mr. CARPENTER. I think, if this answers your question, the working relationship that the Bureau of Diplomatic Security has with the FBO has been extraordinary and, quite frankly, very constructive. If a new organization were created, that relationship would have to be recreated. An understanding of the important elements, ideas, and concepts we bring to the table would have to be transferred. Right now, we have a very smooth working machine. If you were to create a new institution to deal with this, clearly authorities would have to be granted to ensure that this would continue.

Mr. GEJDENSON. Let me ask you a question. Are you familiar with the attack on the Ambassador's residence in Syria some year or so ago and the Ambassador's wife bravely stood in a room there calling people, telling them not to show up to work, and we finally resolved that situation and the Syrians paid us for the damages? How much of your focus is on that Ambassador's residences, employees' compounds? Is that a big challenge for you?

Mr. CARPENTER. It is clearly a challenge. In some parts of the world it is more of a challenge than in others.

I happened to be in Syria 2 weeks after that particular attack, and I saw firsthand the damage that was done, and it does give you an appreciation of what can happen and how quickly it can happen. We have not been of a closed mind or turned our attention away from ambassador residences or the residences of our other employees overseas. It is difficult, quite frankly, when they are dispersed throughout the cities. If they were collocated on a compound, it would be much easier to secure. However, the difficulties in securing these residences vary from country to country.

Mr. GEJDENSON. Is there a balance between—I hear a kind of desire to put them in a compound, but a compound is a much bigger target. You take all your employees, you spread them all over the town, you know, you have got people living amongst the public. That is some danger. On the other hand, there is no one place you can go to get 200 Americans or 100 Americans. What is your estimate on the advantages, disadvantages, or is it country specific? In some countries, it is better to disburse them; and, some countries, it is better to keep them in a compound?

Mr. CARPENTER. I believe it is country specific. In areas where crime is a larger threat than is a terrorist attack, I would suggest keeping them on a compound would be preferable. When you are looking at a terrorist attack, perhaps dispersal would be the better. It is going to be country specific. Quite frankly, we are fully engaged in looking at this issue as we move down the road toward building new facilities. Do we need to collocate on embassy compounds? Do we need to collocate all of our employees on compounds separate from our embassies? Or is dispersal the proper way to go?

Mr. GEJDENSON. I think it is a tough call. I know you obviously spent a lot of time—Mr. Kennedy, what do you think about the relationship between your two organizations?

Mr. KENNEDY. I think the relationship is very good. I think that what we have done over the past few years, which is taking a unit of professional security officers and placing them within the Bureau of Administration's Office of Foreign Buildings where they oversee, monitor and implement the security standards, has worked exceedingly well. That close nexus where they are part of the same organizations and we bring in the construction, the architectural and engineering expertise, and they bring security professionalism, is the way to go. We get fast turnaround. We always get the professional advice we need on scene.

Mr. GEJDENSON. Let me close by saying two things.

Most of the embassies I have been to lately have done an excellent job showing me when I go there their security concerns, their needs, the conditions they are operating under. But I would suggest that maybe one of the things you do is you send out a memo

to our embassies around the world that when a congressional delegation shows up, if they already have it, they ought to put the security issues at the top of their explanation, what their problems are, what changes they have made, so that every Member as they go someplace gets a deeper understanding for this. Because I think it is not just the White House's responsibility, it is our responsibility to make sure we have got an adequate system of protection for our employees, Americans, serving overseas.

Second, maybe the Chairman and I and other interested Members might take a tour of the State Department, take a look at what you are doing there, things you can tell us, give us—some of the stuff I think is better when you see it than just kind of talk about it. Maybe the Chairman and I can get together and pick a date.

I thank the Chairman for his indulgence.

Chairman GILMAN. Thank you, Mr. Gejdenson.

Mr. Smith.

Mr. SMITH. Thank you, Mr. Chairman.

I want to thank our distinguished witnesses for the good work they are doing on embassy security. I think our Committee properly dispatched and fulfilled its responsibilities when we passed the Embassy Security Act last year. It was signed by the President, and it provided a 5-year predictable amount of authorized levels of funding to ensure that there were no gaps, no years that might be leapfrogged, which, unfortunately, look like might have been the case for fiscal year 2000. So I am very glad to see our distinguished witnesses here.

I think we have more in common than some of our Committee hearings, Mr. Chairman, because I think the Administration and these particular individuals are trying to really protect our embassies, to use all available resources to make a difference. So I would like to ask just one or two questions.

Admiral Crowe had testified, and, Secretary Carpenter, you might remember this, when he pointed out that, throughout the proceedings, his Accountability Review Board was most disturbed regarding two interconnected issues, the first the inadequacy of resources to provide security, which, hopefully, is being addressed; and if it is not, if more resources are needed, perhaps you can tell us today, notwithstanding OMB's looking over your shoulder. Second, the relatively low priority accorded to security concerns throughout the U.S. Government and the State Department.

The point was made by Admiral Crowe that there no longer are any more low threat or missions abroad. You pointed this out, Secretary Carpenter, that because of the mobility—of the enhanced mobility of terrorists that every site has to be seen as a potential threat.

How are we addressing those issues? And, again, do you have money—notwithstanding the amount of the request, and we all have the request from the congressional presentation in front of us. We know what we have authorized. Is more money needed or is this the right amount? Is it too little? Please tell us.

Mr. CARPENTER. Shame on me if I came up here and didn't say we needed more money. But, really the answer to your question is twofold.

One, we have received a good injection of funds here, and we are most appreciative of that. But in my professional expertise, if there were an area where we are wanting, it is that we clearly do not have enough personnel to support the mission at hand. And I have testified before, sir, regarding lack of "bench strength" within my Bureau to respond in the event of threats to our posts overseas, we are using the same cadre of people to support every problem we have. Whether it be domestic at the Department of State, whether it be the protection of our foreign dignitaries, responding overseas to emergency situations, it is the same people. And there are far too few of them. This is a process that has been going on for over 2 years in a very, very intense way. I am burning up my people as we go.

We will continue to do our jobs, but without more personnel, my fear is that over the long haul we will fail. These people will wear out and another shoe will drop in another area that is as yet unknown to us.

Mr. SMITH. On that point, if you could just suspend briefly, how many personnel are we talking about and how much money are we talking about? Do you have an estimate?

Mr. CARPENTER. It is difficult to quantify, but we are in the process of preparing, as a result of the top-down study that was done that we discussed last Thursday at the hearing, a strategic plan over a 3-year period asking for somewhere in the neighborhood of about 900 people over a 3-year period. These people come in all disciplines, including special agents, engineers, civil servants, to address our shortfalls in a lot of projects in our counterintelligence arena, our uniform guards program, etc.

Mr. SMITH. Will a request for that be forthcoming from the Department?

Mr. CARPENTER. It is our intention to have this prepared within the next 30 days, and it would be my hope to get it here soon thereafter.

Mr. SMITH. I appreciate that, and thank you, Mr. Chairman. Again I want to congratulate you on an excellent job.

Chairman GILMAN. Thank you, Mr. Smith.

Dr. Cooksey.

Mr. COOKSEY. Thank you, Mr. Chairman; and we thank you for being here. When I walked into the meeting earlier, I walked in and said, gee, these are the same people who were testifying the other day or is it just deja vu? But it is a slightly different topic, but we are glad to have you back. We have gone from State Department to embassies.

I am on the transportation subcommittee that deals with public buildings and domestic buildings in this country and know some of the issues that have come up on our domestic buildings, not State Department buildings, but some of the buildings in the Washington area and around the country, and my line of questioning will reflect that background.

First, Mr. Kennedy, you said that of the contractors who there have been 18 of these buildings or modifications of buildings that have been done by American contractors. Is that correct?

Mr. KENNEDY. We have 18 major efforts overseas that we are using American contractors. For certain small projects—for exam-

ple, Dr. Cooksey, when you are just building iron beams around the perimeter of the embassy, where the local labor and materials are available, it is advantageous to the American taxpayer to use local labor supervised by an American officer from the embassy, using a standard that comes from the Overseas Security Policy Board. So those small projects are done by local——

Mr. COOKSEY. So are any of the major projects done by local contractors or have they all been American contractors, United States?

Mr. KENNEDY. The majority of the major projects are done by American contractors because we want to use American architectural standards, American engineering standards; and we use companies such as Brown and Root and Perini which are under contract to us, because we know the quality is there.

Mr. COOKSEY. What about Bechtel? Have they done any of these?

Mr. KENNEDY. They are not a part of this. Bechtel has worked for us before, sir, but we put out for bid these indefinite quantity efforts, and the two winning American companies were Brown and Root and Perini.

Mr. COOKSEY. When I was in the Air Force many years ago Brown and Root did a lot of construction then. Of course, that was when Lyndon Johnson was President, which is another story.

Is there any consideration to using sort of a standardized, cookie-cutter type of building construction, and is that done?

Mr. KENNEDY. Patsy Thomasson, who is my director of the Office of Foreign Buildings, has a team that is working on that now. There are a certain number of I guess you could say small- to medium-sized embassies around the world which do have almost a standard pattern, sir, an ambassador, deputy chief of mission, security officer, consular section, etc. cetera. So we are looking at that right now to find out if we can come up with an architectural and engineering design that would be standard, and then we would maybe have a different facade on the building, brick one place, stone in another, in order to blend into the local environment. But that is something we are looking at very, very closely because we see advantages both in time and in cost.

Mr. COOKSEY. Well, I think it is important to consider the local environment. I would hate to have all of our embassies look like McDonald's hamburger places. I hate to go to another country and see a McDonald's because that is a sign that the ugly Americans have gotten there before we have. I think that, too often, we go in and try to impose our culture and standards on other countries, and I warn them not to be inundated by Americans, but just so far as the walls, the structure, the security——

Mr. KENNEDY. We have security standards. The walls must be so thick, they must resist so many pounds per square inch. What we do is engage a local architect to work with us on the facade, nothing inside, nothing of a security nature, so that we can blend into the local environment, as you rightly point out.

Mr. COOKSEY. Mr. Carpenter, would you agree that the emphasis on physical security and counterintelligence is a change in the basic RSOs, regional security officers, job or has their job description always been the same?

Mr. CARPENTER. I think that there has been expansion of their duties and responsibilities. If I had to put it in one category, it

would be "outside the walls." We have always been focused on counterintelligence issues. However, what we are involved in to a much greater extent is relationships with host government officials, local police authorities, and local military authorities.

An RSO under duress needs to be able to pick up the phone and get the person that he knows can respond. In years gone by, the RSOs' responsibilities basically were confined "inside the walls." We will lose if we don't extend our reach outside those walls. The countersurveillance program that we have talked about is a major step in that direction. It gets "eyes and ears" outside the embassy, one block, two blocks, or three blocks away and forces us to engage more with local authorities. It forces an RSO to get out of an embassy and make these contacts that would be needed in the case of an emergency.

Mr. COOKSEY. Good. Well, the State Department security people that I have had some contact with on CODELs are professionals, that I know are good people, but still they were apparently confined to the area within the walls. They need someone with your background and your expertise, and I am encouraged to hear that.

With the increase in Diplomatic Security positions you have been able to provide posts with assistant RSOs, but are you sending out assistant RSOs with different skills to augment these people? And are these RSOs former Secret Service personnel or are they former State Department security personnel? For example, computer security, electronic security. Who has the most expertise and who is doing that, Secret Service personnel or former State Department security personnel?

Mr. CARPENTER. The Bureau of Diplomatic Security has a mix of special agents, engineers, technicians, and computer experts. We have also used former Diplomatic Security agents temporarily. Clearly, and coming from the Secret Service I can say this firsthand, Diplomatic Security has the most knowledge of how to work in an overseas environment of any Federal law enforcement agency. None of the others are even close—and I think other agencies would testify to that reality.

The agents that we have sent out come up through the system. We have more senior agents at the larger posts where the programs are more demanding. They have assistants who work for them. But all receive a substantial amount of training in the appropriate fields and disciplines that they will be required to use overseas.

Mr. COOKSEY. Good. I have been impressed with the professionalism of the people in the State Department and favorably impressed. I am concerned sometimes that the political appointees don't have the background, the expertise or the—they are good people, well-intentioned people, but are a little naive, somewhat naive when it comes to these security considerations, and I hope that they come up with some level of understanding there.

I used to work in Kenya and East Africa doing—quite frankly, doing eye surgery. I am very sensitive to that issue. You know, as you well know in Kenya, there was a small bomb detonated, the people ran to the windows, looked, and most of the injuries that occurred were eye injuries. I know one surgeon that works at a Presbyterian hospital that I did 8 or 10 cornea transplants in about a

24-hour period 1 day, and he was involved in taking care of those, and it is a very sophisticated hospital for that part of the world.

I gather from your comments that you are really taking major measures to prevent flying glass and blinding injuries.

Mr. KENNEDY. If I might, that is one of the things that we are most concerned about. We are pursuing this on two tracks. As Admiral Crowe's report so rightly recommended and as the IG has pointed out as well, if the structure of the building is sound enough for us to put in laminated windows and heavier frames, we do that. At the same time if the building structure isn't good enough, when the blast goes off what will happen is the entire window, the entire big piece of laminate in the frame, will go flying through the room like a sieve, wiping out the people in front of it.

Mr. COOKSEY. So it's bad either way.

Mr. KENNEDY. Yes. But what we do is we have gone to laboratories like Sandia National Laboratories and to the private sector and we have doubled the strength of what is called shatter-resistant window film. In fact, it is plastic wrap that is used now—we used to use 4-millimeter thick. We have now doubled that to 8-millimeter strength. We are applying that to all the windows on all of our facilities. We will have that done by June of this year. When the blast goes off, the window shatters, but this 8-millimeter film holds the glass shards together, and you get the whole window, the glass part in effect, plopping down into the room without any damage.

In one of our posts in the newly independent States about 6 months ago a bomb went off, not directed at us but at a neighboring facility, and after the bomb went off many of our windows shattered, but the entire window was still intact because the plastic had done exactly what it was supposed to do, not injure our personnel.

Chairman GILMAN. The gentleman's time has expired.

Mr. Chabot.

Mr. CHABOT. Thank you. I had another committee so I apologize for not being here, and you may have already answered my question. So I will apologize in advance for that if you already did.

My question is just about the overall—I know we have many embassies all over the world, and of course since the terrorist attacks some time ago our concern about this has been elevated even higher than it always was about the safety of our people and the other folks working there. How many of our embassies just—and you don't have to specifically name which ones—but how many of our embassies still really need to be dramatically improved relative to security measures? In other words, do we still have some that are out there that may be fairly easily attacked or come under some sort of successful terrorist attack? And, again, we don't want to broadcast which ones they might be, for obvious reasons, but either a percentage or just some—without giving specific examples, could you comment on that?

Mr. CARPENTER. Yes, sir, I would be glad to. About 85 percent of our embassies still do not meet the 100 foot setback standard that is critical for protection against a large vehicle bomb. Set back is really the best protection, and we do not have that in 85 percent

of our embassies on one or more sides of the building. They may meet it on three sides, but one side remains vulnerable.

Mr. CHABOT. Can I followup on that then. How does one then go about obtaining that goal? Do you have to buy up buildings around there and literally tear them down? Is that what you do or what?

Mr. CARPENTER. It is a combination of those things. We have bought and torn down buildings in some instances. We bought adjacent buildings when buildings were available. We have also bought parks. We have bought gas stations. We have bought empty lots in an attempt to obtain the setback. Long term, the solution is to move the facility to a site large enough for the setback.

Mr. CHABOT. And then if you do move to another site—I mean, at what point do you run into the problem where, you know, it is more of a—some sort of fort as opposed to an embassy where people can easily come in and do business with the representatives of the U.S. Government in that particular country? I presume that is a fine line you are always walking in these matters.

Mr. CARPENTER. It is a fine line. But let me assure you, we have no intention of building forts or prisons or military bases. We think you can attain an aesthetically attractive building, and still have it be secure.

Mr. KENNEDY. I would just say, sir, in response to your earlier question, we have already acquired 87 properties around the world at 25 posts, and we are now negotiating on 31 others at 14 posts. So we need to push that back. I think that if you use clever design work you can create a facility that is safe but inviting, and we are partnering with a large number of American architectural firms, some of the best, and are also engaging at every post where we are doing this one local architect who knows the local culture and the local environment, and he or she works on the outside of the building, never on the inside where there would be technical security issues.

But I think there are cases such as Lima, Peru, for an example, where we have built an inviting building, created the perimeter but creating sort of controlled pathways for people to come in from the walk to the consular section or the public diplomacy section. It is not easy, but if you get the right architectural and engineering support we can do it.

Mr. CHABOT. Thank you very much. Appreciate it.

Chairman GILMAN. Thank you, Mr. Chabot. I have one or two questions, and then I will call on Dr. Cooksey for a few more.

Mr. Kennedy, FBO is ready to begin construction on their new embassy in Luanda, Angola. However, that will require waivers for not meeting the 100 foot setback on all sides. That seems to be setting the wrong precedent for these important standards. Has the FBO searched for a larger plot of land to allow for full setback?

Mr. KENNEDY. Mr. Chairman, this is one of the knottiest conundrums. We have been searching for a larger part of land in Luanda, Angola, for 5 years. We have simply not been able to find a plot of land that would give us the full 100 foot setback on all sides.

Our people in Luanda now, some of them are literally working out of trailers where, you know, a firecracker might blast the walls of the trailer down. So we, in full consultation with Diplomatic Se-

curity, have been measuring this. Given that we have in effect an F in security in Luanda and we can move—potentially move with waivers to A minus or a B plus, we figure, though that does not meet everything, the movement from F to A minus without regard to any precedent it is setting would be in the interests of both the U.S. Government on the whole and our people there in particular.

Chairman GILMAN. What kind of a setback would be available at the land you are looking at?

Mr. KENNEDY. We would have a 100 foot or so on two sides and over 65 foot on two sides. So it is significantly better than we have now.

If I might add one other thing, Mr. Chairman, the standards that come from the Overseas Security Policy Boards say a 100 foot setback and a concrete wall of so many inches thick for yield blast resistance, and that is a formula: 100 foot plus concrete equals safe setback. What we would do on the two sides that are 65 foot is to increase the thickness and the strength of the concrete wall. So you, in effect, have exactly the same setback effect by simply increasing the thickness and the strength of the concrete.

Chairman GILMAN. You will be doing that in the front wall as well?

Mr. KENNEDY. Yes, sir. So we would achieve the same goal by using more concrete and less footage.

Chairman GILMAN. Mr. Carpenter, there are incidents where American government employees in Inman-qualified embassies are being allowed to move off the embassy space, thereby creating new security concerns and security challenges. What is your view on permitting employees to leave the Inman embassies for less secure facilities and who is granting waivers for that kind of movement? Are you being consulted?

Mr. CARPENTER. Mr. Chairman, I am not aware of the specific facility to which you refer. I would, quite frankly, not want to hear it in this hearing.

Chairman GILMAN. If I may, it is USAID in Bogota.

Mr. CARPENTER. USAID in Bogota? Unfortunately, the most I can tell you is that proposal is under review. Quite frankly, I am not aware of the specifics of that request on AID's part.

Chairman GILMAN. We would hope you would take a look at that and let our office know.

Mr. CARPENTER. I would be glad to.

Chairman GILMAN. Is that a generally good idea, when we are being asked to fund so many security projects already, of allowing the movement?

Mr. CARPENTER. Again, Mr. Chairman, that is a decision that is country and post specific. In some places, dispersal of our employees is, in fact, a security enhancement. One of the realities, even with an Inman building, is they may be limited in functionality, and sometimes very hard decisions have to be made. However, let me assure you, before we would move someone out of an Inman-style building, we would have to have reasonable assurances that what they were moving to would provide them maximum security.

Chairman GILMAN. Ms. Williams-Bridgers, do you agree with this proposition of allowing such movement?

Ms. WILLIAMS-BRIDGERS. I do agree with Assistant Secretary Carpenter that it has to be a country specific decision.

But certainly one of the greatest challenges that FBO and the Department have faced in building new embassies overseas or making major renovations to accommodate increased staff is the accommodation of other agencies' requests for either movement off the compound or for increasing their staff.

We saw this in Moscow when other agencies throughout the course of the construction decided on significant increases in their staff and it made for major reconsideration of configuration of space in the embassy. We shall see this in many other instances. So whether or not FBO continues to maintain the functions as presently structured or if those functions are assigned outside of the Department of State, the "right sizing" of mission staffing is going to have to be a primary consideration of the new unit held responsible for designing and constructing new embassies. Interagency communication will be essential during the design phase of future embassy facilities.

Chairman GILMAN. Madam Inspector General, your statement indicates that the Department spent $77 million in fiscal year 1999 on the surveillance detection program. Does your initial assessment of the value of that program support that kind of an expenditure and can that level or more be sustained over time when there are so many demands for costly physical upgrades?

Ms. WILLIAMS-BRIDGERS. I think it is important to note that as we have focused our attention on the need for physical security improvements in our embassies overseas that there are a number of other initiatives, including procedural security initiatives and information and intelligence gathering, that are as important in contributing to our ability to protect Americans overseas where they live and work. The surveillance detection program improves our ability to collect information about those who may potentially harm our employees in the embassy. I think there are improvements that need to be made in the surveillance detection program.

Currently, the principal objectives of the program are to collect information about those that might be watching us in the embassy and to engage local police services, local guard services to spread our eyes and ears outside the embassy compound. I think it is most important for us to now begin using that information more smartly, sharing the information regionally with those that can better assist us in identifying who the potential terrorists are and then identifying what kinds of assertive action we might take to pursue those individuals, beyond just the mere photograph and the recording of their name and a photograph.

Chairman GILMAN. Thank you.

Dr. Cooksey.

Mr. COOKSEY. Thank you, Mr. Chairman.

Mr. Carpenter, I have got two questions I want to ask you and would like you to answer them in 60 seconds or maybe give us a written explanation, because I don't want to totally ignore Ms. Williams-Bridgers.

It has been brought to my attention that there is an embassy that was actually checking vehicles inside the embassy gates and didn't have any type of operational delta barriers to prevent this

type of access to the compound. Is there a standard operating procedure for inspecting vehicles and has this been reiterated to the basic security people?

To elaborate on that, I was at an embassy last year in a part of Asia and—good people, but, I mean, the embassy is right out on the street. There is no security, and there is really no way to check. There is not even a perimeter there. I mean, it is on the main street. That is one question.

No. 2, does DS believe that it can do most—should there be some risk analysis made so you can make some informed judgments about the spending priorities with this limited amount of money?

Mr. CARPENTER. With regard to vehicle inspection, yes, sir, there is a standard procedure. I think I was just at that same embassy 2 weeks ago that you have had the occasion to visit and was appalled when I saw it.

The reality is that we have to play the hand we are dealt, and we have had to do some things in nontraditional ways. Sometimes that includes sweeping the vehicle after it is inside the gate. That is not our SOP, but we felt it better to sweep it even though it is inside the gate than not sweep it at all. We can't close the necessary streets or obtain a location reasonably close by in which to do these inspections.

Part of the reason for having a countersurveillance program is to try to give us a virtual setback. That program gives us a span of control outside the embassy. It gives us early warnings of impending problems and the ability to alert a facility that a problem is coming.

We have been dealt a bad hand when it comes to setback. As I said earlier, 85 percent of our facilities don't have it. We are trying to make adjustments and accommodations to the best of our ability. We are going to have to continue to change the way we are doing business out there.

What we have in place is good now. Next month, it is going to be better and the next month even better; and certainly a year from now, assuming we are still in those safe facilities, it is going to be even better, still.

Mr. COOKSEY. Good.

Ms. Williams-Bridgers, I was on the IG team the last 6 months I was in the Air Force so I know that all IG people aren't terrible, ruthless people, but the job has to be done. In my capacity on the Public Buildings Subcommittee of Transportation we found that there was some buildings in this country, domestic again—of course, this is a domestic issue—that were built, one as many as 30 years ago or 27 years ago for probably 50 to 70 million dollars, I forget the exact number, but over the years the lease payments for that building are approaching $900 million and nearly a billion dollar. Do we own all of these buildings abroad? Do we own all embassies or are, in fact, some of them leased out?

Ms. WILLIAMS-BRIDGERS. I will defer to Assistant Secretary Kennedy. However, we do not own all of our overseas property holdings.

Mr. COOKSEY. There was some political patronage. Does it carry over into our embassies? That is ultimately my question.

Mr. KENNEDY. Dr. Cooksey, I don't think it involves political patronage so much as the lack of a capital program. If you take——

Mr. COOKSEY. You remind me of Congress, for giving me your money, should—I will quote Admiral Crowe who says, there's enough blame to go around between the Legislative and Executive Branches. I will blame it on Congress.

Mr. KENNEDY. We have some 12,000 buildings overseas. We probably own less than 2,000 of them.

Mr. COOKSEY. Really.

Mr. KENNEDY. Basically, we try to own wherever we can. But, in many cases, because the funds available to us are simply enough to pay the rent but not enough to make the up-front payment that is needed to purchase, we are stuck—just as you pointed out from your experience on your other committee, we are stuck paying the rent every day.

That is something that the overseas presence panel pointed out. It is something we are working with under Ms. Thomasson. We are in constant consultation with OMB to see if there were some way to move this along so that we could lease to own or do some new, inventive, creative way of funding and financing which would not be an immediate burden on American taxpayers but would put us in a very different position 10 years down the line.

Mr. COOKSEY. From a total long-term cost standpoint, we would be better off to own these buildings.

Mr. KENNEDY. Absolutely, sir.

Mr. COOKSEY. I want to make one other closing comment. I made this to a Republican colleague the other day, and I put him on the spot, and I apologized to him, but it is a message that I still want to put out, and it is marginally related to this Committee.

I think one of the most disgraceful, cowardly, despicable acts of omission that is going on right now by members of both parties, the Executive Branch, maybe the State Department, is the fact that we are totally ignoring the human rights abuses that are going on in Africa. I am talking about Rwanda, Burundi, today Sierra Leone. A good friend of mine had a wonderful eye clinic with wonderful equipment there that is destroyed. And Eritrea, Ethiopia and now Zimbabwe, places where they are going in and slaughtering people, cutting children's hands and legs off. We are focused on human rights abuses in China, and they have got abuses there but not on this scale. I think that the politicians in this city who don't have the courage to stand up to these human rights abuses when they are diverting attention to China should be held to account for it.

My question, in these countries I mentioned, Sierra Leone, where they cut the children's hands off and feet and legs, in Rwanda and Burundi and more recently in Zimbabwe, where they are shooting people, and today I read in the paper they are taking a lumber company out, what kind of security do we have there for our embassies and are the embassies able to take a position there? Is the fact that we have got a bunch of cowardly people in this city a reflection of the fact that we don't have embassies there or security there that could address this really despicable, cowardly act of omission by the people in this city?

That would be a good one for you, Ms. Williams-Bridgers. I didn't mean to ignore you on the other questions, but I am concerned

about this. Is it because we don't have the embassy personnel, the security in these countries?

Ms. WILLIAMS-BRIDGERS. We do have an American presence in the many of the places that you mentioned, and I couldn't agree with you more that there is no more despicable act than what we see commissioned across too much of the globe as the abuses against human beings, against women and children who are virtually defenseless.

The security of our embassies and our embassy personnel are established, first and foremost, to protect Americans who are working and living to support the business of the American embassies abroad. The mission of our embassies abroad is to advance human rights issues in many of those locations, and I don't believe that it is being ignored at all by the Department of State, and its best efforts are being put forward.

That said, we haven't looked specifically at the advancement of human rights policies by any of those particular missions that you have mentioned in the course of recent inspections.

Mr. COOKSEY. My question then, in summary and in closing, Mr. Chairman, if in these countries we had a state-of-the-art embassy in terms of construction security, could we have a more effective presence in addressing these human rights abuses against women and children? That is who the abuses are against. I have delivered babies with women who have had female genital mutilation. I have taken care of people with land mine injuries and AK–47 injuries, some years ago, 8 or 10 years ago. But could we do a better job of addressing these problems if we had this state-of-the-art security in our embassies that you are talking about or could we not?

Ms. WILLIAMS-BRIDGERS. There is absolutely no doubt that without the adequate facilities, without safe facilities to house U.S. Government employees who are working overseas to advance issues like human rights that we cannot effectively execute our mission. I think that it is why it is one of the first and foremost priorities of the Department to ensure that we have the commitment of funding, that we have all of the resources that are necessary to enhance the security and, therefore, the viability of our missions overseas.

Mr. COOKSEY. Thank you, Mr. Chairman.

Chairman GILMAN. Thank you, Dr. Cooksey.

One last question, Mr. Carpenter. The case that Dr. Cooksey mentioned in the South American embassy, that delta barrier, I have been informed, in front of the vehicle being checked inside the compound was not working. The next stop was the front door of the Ambassador's residence and the chance for a suicide bomber. Has that delta barrier been fixed since that inspection?

Mr. CARPENTER. They are still working on it. Like a number of other issues out there, we are aware of the problems that we have. That clearly is one. Equipment is sometimes slow to be installed. It is critical that it be installed. They have taken some other measures to mitigate the threat until it is installed; but unfortunately, I have to report that it has yet to be completed.

Chairman GILMAN. Our Committee called this to your attention several months ago. We hoped that that would be taken care of properly.

Mr. CARPENTER. I wish it had been. It should have been.

Chairman GILMAN. I want to thank the panelists for your time. Committee stands adjourned.

[Whereupon, at 11:52 a.m., the Committee was adjourned.]

A P P E N D I X

MAY 11 AND MAY 17, 2000

Statement of The Honorable Benjamin A. Gilman
May 11, 2000
Current Challenges to State Department Security

Good morning. Today our Committee examines "Current Challenges to State Department Security."

The nature of these challenges is not a mystery. Over the last two years, there have been numerous, well-known serious security failures at the State Department.

In 1998, a man in a brown tweed coat grabbed highly classified documents from an office in the Secretary of State's suite. The man and the documents have not been found.

Last year, a Russian spy was discovered outside the Main State building listening to a bugging device planted in a seventh floor conference room. And of course, last month saw the revelation of a missing laptop computer that contained highly classified information. The laptop has not been found.

Again in 1999, we were told that a computer software program written by citizens of the former Soviet Union was purchased by the State Department on a sole-source contract and installed in posts throughout the world without the proper security and vetting procedures. The program had to be removed from every post. To this day, we have not received an explanation of why and how this happened.

The news media has extensively covered each of these events. What is less known, however, is that officials at the State Department have known for years that security at the State Department was vulnerable to just these kinds of incidents.

At a March 1998 State "town hall meeting," Undersecretary for Political Affairs Thomas Pickering called a "Department-wide wake-up call" about security issues. Another top official noted that promoting individual responsibility will require more security training and "rigorous follow-up." Very true.

Later that year, a report by the Inspector General highlighted problems in the Bureau of Intelligence and Research (INR) at State and made recommendations to fix them. Today, INR has not yet responded to that report.

Another report by the Inspector General in 1999 recommended broader changes in State's security policy, including the transfer of authority over "codeword" level material from INR to the Diplomatic Security Bureau. Although this report was issued in September 1999, its recommendations were at first rejected by the Department; they were not adopted until April 2000, well after the celebrated laptop was found to be missing.

On November 17th, 1998, a new State policy requiring escorts for all visitors was

announced. It requires "all visitors with the exception of active U.S. Government agency personnel who display proper photo identification shall be escorted at all times." Six days later, the policy was rescinded. Nine months later, it was re-implemented.

Just last week, the Secretary of State held another department-wide Town Hall Meeting on security matters. While her tone and words were appropriately tough, we cannot help but wonder if they will have any more impact than those of Mr. Pickering and other top officials at the 1998 Town Hall Meeting.

A few days before the most recent town meeting, the Secretary issued a document that revealed, on close analysis, that it had decided not to measure its security performance on the basis of the number of security compromises detected. In addition, the Department failed to make progress on reducing a scandalous backlog of security reinvestigations. It now moving toward, in effect, a FIFTEEN YEAR cycle for security updates, rather than the FIVE year government standard.

The Department did, however, manage to significantly exceed the target it set for itself in reducing its inventory of overseas vehicles over five years old. So we are left to ask: are the Department's priorities proper? Should we be surprised that a casual attitude toward security is part of the Department's culture if its budget priorities practically shout that information security is not a concern?

We have learned that despite recent changes in security policy, reporters from foreign news media have access to many parts of the Main State building without any supervision. Indeed, we are informed that press personnel with identification cards have 24 hour access to the building, including weekends and holidays.

In other words, the new escort policy has a hole you could lead an elephant through. It is no secret that foreign intelligence agencies use reporters as agents. During the Cold War, KGB agents routinely used reporters' credentials as cover for their activities.

The recent book, "The Sword and the Shield" by Christopher Andrew and Vasili Mitrokhin details numerous incidents of Soviet spies posing as reporters. It is a safe bet that the KGB's successor agencies in Russia today use the same techniques.

No security policy at State will be adequate until foreign journalists are appropriately escorted, just like other visitors, beyond the normal press areas.

A secure State Department, however, is not just a matter of changing a few policies. It is the daily culture of our diplomats that must change. Every person in the State Department from maintenance personnel to Ambassadors to the Secretary of State must reprioritize and make security a top concern.

This does not mean that policy-makers in top jobs are off the hook, far from it. Leadership must come from the top, and the responsibility for the current, disastrous condition of State Department security lies with the Secretary and her top aides. I would like to quote from an anonymous letter received by the committee just this week from a foreign service employee:

"For the poor security environment at the U.S. Department of State to improve only one thing is required, that being for State to seriously and publicly punish several senior officials (including at least two current ambassadors) for security violations. The punishments would have to be real and hurt, to include firings and criminal prosecutions."

I trust that the Department of State, and we have several of its top officers here today, will give this advice great consideration. Our nation cannot tolerate any further security violations at the State Department. Department officers need to realize that both the lives of innocent people and the national security are put at risk when they are haphazard at following elementary procedures.

The consequences for compromising national security secrets, whether intentional or inadvertent, are great. They result in costly investigations, damaged relations with other nations and, most gravely, possible mortal danger for Americans who serve our nation abroad.

In closing, I'd like to quote a former Ambassador to the United States from France, Jules Cambon, who said, "The day secrecy is abolished, negotiation of any kind will be impossible."

It is no exaggeration to say that the very mission of the State Department, to carry out our nation's foreign policy, is today in peril.

STATEMENT OF JACQUELYN L. WILLIAMS-BRIDGERS INSPECTOR GENERAL OF THE U.S. DEPARTMENT OF STATE AND THE BROADCASTING BOARD OF GOVERNORS

FOR THE

COMMITTEE ON INTERNATIONAL RELATIONS U.S. HOUSE OF REPRESENTATIVES

MAY 11, 2000

Mr. Chairman and Members of the Committee:

Thank you for the opportunity to testify before the Committee on the Department of State's (Department) security programs as they relate to the protection of sensitive intelligence and national security information.

Since the August 1998 bombings of the embassies in Nairobi and Dar Es Salaam, the Office of Inspector General's (OIG's) oversight of the protection of our people, information, and diplomatic facilities has become an even more critical mission. I have created multidisciplinary teams in OIG to evaluate the implementation of many physical security initiatives and the expenditure of $1.5 billion in the emergency security appropriation. By the end of fiscal year 2000, OIG will have evaluated the physical security and emergency preparedness of 68 embassies since the bombings. In addition, we are now completing the final in a 6-year series of reviews of the new Secure Chancery Facility in Moscow, and we are monitoring progress in the construction of an annex to our embassy in China.

The Department has implemented a diligent and effective strategy to enhance the physical security of our overseas missions, and today U.S. missions are significantly more secure than they were 18 months ago. Our embassies generally do a good job of protecting classified information, including our classified computer systems.

Recent security lapses at Department of State Headquarters facility (Main State) in Washington, D.C. clearly demonstrate that attention must be given to address vulnerabilities in protecting vital information on the domestic front identified by OIG last year.

The Secretary's April 24 decision to transfer authority for protection of sensitive intelligence related material from the Bureau of Intelligence and Research (INR) to the Bureau of

Diplomatic Security (DS) implements critical corrective actions that we recommended as essential to ensure proper safeguards for our most sensitive intelligence related information.

In my statement today, I will discuss the specific deficiencies that have perpetuated a lax security environment in the Department of State and that OIG identified during the course of our security oversight reviews. The Department has implemented about 77 percent of the security recommendations we have made from 1997 to 1999.

In summary, OIG has found:

- Ineffective access controls in the Department left offices vulnerable to the loss or theft of sensitive information and equipment by unescorted, uncleared visitors and contractors.
- Lack of adequate physical and procedural security measures in offices resulted in classified documents not being properly controlled and accounted for.
- INR was not fulfilling its security function, and unit security officers in other bureaus were not enforcing security requirements, and
- Disciplinary actions for security violations did not serve as a deterrent in correcting poor security practices.

Although the Department has begun to address these specific physical and procedural security problems, what is truly needed is continuous vigilance by all Department personnel with an ongoing commitment to maintain and enforce the highest level of security awareness and compliance.

Background

State OIG is unique among Inspectors General in that in addition to all of the traditional IG functions of audit, inspection, and investigation, we also have a multidisciplinary office that focuses exclusively on security and intelligence oversight. This gives me the tools I need to exercise my special responsibilities for the security oversight of all U.S. Government personnel overseas (except those under our regional military commanders). In performing this function, OIG has enjoyed more than a decade of strong support from the Director of Central Intelligence through our partnership with the Center for Security Evaluation.

As you know, following several disturbing incidents, most notably the February 1998 incident where an individual wearing a tweed jacket removed sensitive documents from an office in the Secretary's suite, my office was directed by the Senate Select Committee on Intelligence to "...conduct a review of State Department headquarters' policies and procedures for handling classified information and submit a report to appropriate committees of Congress with any needed improvements..." Our report, issued in September 1999, was entitled *Protecting Classified Documents at State Department Headquarters (SIO/A-99-46).*

Most of our recommendations in that review have not been fully implemented, but the Secretary's recent decision to transfer authority for the sensitive protection of intelligence related material from INR to DS addresses a key recommendation. In addition, the Department has told us that it has initiated plans to implement a majority of the remaining OIG recommendations.

I will now discuss the deficiencies that OIG has identified in the following areas, and I will present the Department's responses to our recommendations:

- Access controls at Main State
- Controlling classified documents
- Information security
- Human resources and security management
- Security incidents, disciplinary actions, and investigative referrals

Access Controls at Main State

The Department handles, processes, and stores thousands of classified documents each day at overseas posts and at the Main State headquarters facility. Countless meetings are held where classified information is discussed. Gathering, analyzing, and distributing sensitive intelligence information is central to the Department's mission to implement U. S. foreign policy. Regardless of the means by which information is disseminated, it is essential that the disclosure of such information be limited to authorized personnel with a need-to-know and appropriate security clearances who have been adequately briefed on policies and procedural requirements for protection of such information.

Visitor Access

In August 1998 when we began our review of the effectiveness of Department policies and procedures for protecting classified documents at the Main State Headquarters facility, the Department policy allowed visitors to move about unescorted once they demonstrated to a guard at one of the perimeter entrances that they had valid business in the building. These visitors were unaccompanied even when proceeding to areas where classified information was handled, processed, and discussed. A significant number of these visitors were foreign government officials. OIG concluded that such access posed an unnecessary security risk and that greater control over the movement of all visitors was needed.

The Department instituted, in August 1999, a new visitor escort policy that requires all visitors who do not possess a valid U.S. Government identification card to be escorted at all times while in the Main State headquarters facility. This is an excellent first step, and we will report back at a later date on the implementation of and compliance with the policy.

Char Force and Contractors

In response to OIG's recommendation, the Department issued a notice in December 1999 reminding supervisors that all uncleared cleaning and maintenance personnel must be escorted

when working in classified work areas. The Department has begun reviewing all contractors assigned to the Department to determine which contractors require cleared employees and whether contractors are complying with this requirement. We believe the Department is making a serious effort to eliminate this vulnerability.

Press Access

While OIG supports the new escort policy, a continuing concern is that members of the media (foreign and American) are provided permanent building badges. These identification cards are coded to allow the press personnel access to any of the card readers at Main State's perimeter entrances. The Department's longstanding policy is to allow press personnel with identification cards 24 hours access, including weekends and holidays. OIG remains concerned that the identification badges provided to press personnel presents an opportunity for the badge holder to gain unauthorized access to other areas of the Main State headquarters facility.

Office in the Secretary's Suite

Even the Secretary's suite suffered from many of the same access control deficiencies before the February 1998 "man in the tweed jacket" incident. Before 1998, the suite was accessible to any of approximately 20,000 employees and contractors, other agency employees, and their guests who had identification badges programmed to grant access. During the audit OIG observed that two doors programmed for more restricted access were routinely propped open. The card readers installed at that time were not reliable for tracking who entered or left the suite and the alarm system was not adequate and did not always work when tested. Maintenance, repair, and cleaning personnel were not escorted, and there was no professional security officer assigned to the Secretary's suite.

To the Department's credit, considerable improvements were made following the "man in the tweed jacket" incident. A new card reader system that can track access was installed in the Secretary's suite and throughout the building. Unlimited access to the suite was limited to individuals who routinely work in the Secretary's suite, and there is now a 24-hour guard post. Maintenance, repair, and cleaning employees are reportedly escorted at all times, and DS assigned a professional security officer to oversee the enforcement of security requirements in the Office of the Secretary.

Controlling Classified Information

The protection of Sensitive Compartmented Information (SCI)--highly classified intelligence related information--received by INR requires more stringent safeguarding than documents at the "secret" or "top secret" levels. For SCI facilities, Director of Central Intelligence Directive (DCID) 1/21 requires badge systems to verify identification and authenticate that person's clearance for access. This requirement is being addressed by the Department.

---

[1] *Audit of the Secretary of State's Protective Detail (SIO/A-98-27). The overall objective of this audit was to evaluate the protective security provided to the Secretary by DS.*

SCI facilities (SCIFs) must be protected either by visual control or personal identification authentication. Authentication can be achieved by the use of personal identification numbers in conjunction with encoded badges or by personal identity verification, known as biometrics, which identifies the individual by some unique characteristic, such as hand geometry, fingerprints, and "voiceprints," unless the area is under constant visual control during duty hours. We recommended, and the Department agreed, that biometric devices should be installed at SCI facilities and other sensitive offices. DS has agreed to use biometrics equipment, but installation of a system has been delayed by technical difficulties. In the interim, DS will install an enhanced access system using personal identification numbers.

DCIDs require more stringent physical and procedural security measures for protecting SCI than for other classified documents. OIG found that the Department was not complying with DCID requirements. SCI material was regularly introduced into offices that had not been accredited for the handling or discussing of SCI, and documents were not always properly stored or accounted for. INR had not complied with required routine inspections of 140 Department offices where SCI was maintained. Although not specifically required, none of the offices had received technical surveillance countermeasure inspections to determine whether listening devices had been implanted in any of the offices.

INR informed us in March 2000 that it was visiting each office where SCI is handled or discussed and that physical and procedural improvements for each secure work area will be identified on an "expedited" basis. We responded that the OIG would close these recommendations when the Department:

- Converts each of the "temporary" secure work areas into fully secure facilities in conformance with DCIDs,
- Ensures that sound attenuation standards are in place where briefings of SCI material occur, and
- Verifies that "read only" rooms are actually that, and SCI is not stored, processed, or discussed there.

Our review also found that while SCI documents were distributed to 46 offices each morning, controls or procedures were not in place to ensure that all the material was returned to an SCI facility and properly secured at the close of business. INR did not verify that all the documents were actually returned. All too frequently documents were not returned as required. While we realize document control procedures can be a daunting and tedious task, verifiable control of SCI material is essential.

To address the document control deficiencies, INR advised us that a specialist from the intelligence community would be made available to the Department to establish a sound document control program. The Secretary recently stated in her February 3, 2000, report to the Congress that increased staff and funding would be made available for this purpose. We will be

vigilant in monitoring progress made over the coming months and determine whether positive control of SCI has been established.

Information Security

The Department of State relies heavily on the use of automated information systems for both classified and unclassified communication and to store and process data that is critical to supporting the agency's mission. The data used in these systems is often classified or sensitive and is an attractive target of opportunity for organizations and individuals alike desiring to learn about or damage the Department's operations, or seeking monetary gain. For example, personnel information concerning approximately 30,000 State Department employees could be useful to foreign governments seeking to build personality profiles on selected employees. Further, unauthorized alteration of data in the Department's Consular Lookout system could enable dangerous individuals to enter the United States.

Since its formation, the OIG has done considerable work on both information management and information security. Recognizing the critical role that security issues play in the information technology arena, OIG has realigned its resources to focus on emerging information technology issues. My office has consolidated its information technology and its longstanding information security efforts and created a single Information Resources and Security Management Division (IRSM) in the Office of Audits. The IRSM Division will address emerging issues of congressional interest in five areas: information management, telecommunications, information security, information technology human resources, and information warfare. The strategic objectives are to ensure that:

- Potential cost efficiencies and opportunities for streamlining information management activities are identified and best practices shared,
- U.S. personnel, facilities, information, and material are more secure through the identification and correction of security weaknesses and deficiencies, and
- Systemic weaknesses in information systems and security management are reduced.

My office is currently developing a 3-year strategic plan to identify audit work in line with these objectives.

Over the past few years, OIG audits of the Department's classified and unclassified computer systems have identified numerous vulnerabilties that we have worked with the Department to correct. Among a number of actions taken, the Department has assigned the Chief Information Officer the responsibility and full authority for ensuring that the agency's information security policies, procedures, and practices are adequate.

Last November, OIG issued an audit report on Overseas Telephone Systems Security Management that raised concerns about widespread access by Foreign Service national employees to our sensitive but unclassified networks and our telephone switches.

Further, as part of OIG's audit of the Department's financial statements, we assessed the security controls on the Paris Accounting and Disbursement System. We found that the four main servers at the Paris Financial Service Center were highly vulnerable to penetration by unauthorized internal system users. In addition, we found that passwords governing access to the Paris Accounting and Disbursement System were easily compromised because of weak password administration procedures. In response, the Department has upgraded all of its servers and clients at the Paris Financial Service Center to a more secure configuration and has installed a password filter which requires that passwords be at least eight characters long and contain a mix of letters, numerals, and non-alphanumeric special characters.

OIG is currently reviewing the Department's critical infrastructure protection plan to determine the extent to which it meets the requirements of PDD- 63. As part of our assessment, we are evaluating information assurance and critical infrastructure protection issues affecting the Department domestically and overseas, and those affecting host countries and governments. Further, we plan to determine whether the Department is adequately balancing agencywide security risks--here and abroad--against the estimated cost of its critical infrastructure requirements. We plan to complete our review of the Department's critical infrastructure plan by the end of June 2000. OIG will use the results of our critical infrastructure review as the foundation for our discharge of oversight and reporting responsibilities that are incorporated in the proposed legislation of S 1993, Government Information Security Act.

Human Resources and Security Management

We are encouraged by recent initiatives to strengthen physical access and document controls. There are, however, two areas of security management that continue to concern us: personnel security and unit security officers.

Personnel Security

In our 1998 review of the management of SCI access[2], we found that INR was not effectively discharging its responsibilities to ensure the protection of SCI. Specifically, we found that INR had not complied with the DCID requirement that only individuals with a need-to-know have access to SCI materials and that the results of background investigations be considered in making that determination.

Additionally, the Department lacked formal, documented policies and procedures for granting and terminating SCI access. INR did not have a reliable tracking system to determine when an individual's need-to-know had ceased so that SCI access could be terminated. For example, one individual deceased for over two years was still listed as having SCI access. INR relied on a manual review of the *State Department Magazine* rather than formal personnel records to identify employee transfers, resignations, or deaths. The Director General has agreed to assist INR with establishing a procedure to notify INR of the transfer or termination of personnel, however, the procedure has yet to be established.

[2] *Audit of the Management of SCI Access, (SIO/A-98-49)*

DS conducts the investigations of personnel requesting SCI access and makes a recommendation to INR to grant or deny access. In a random sample of 100 INR security case files, we found that 60 did not contain a DS recommendation. In our view, DS assessments as to suitability should be the overriding consideration in the final determination of whether to grant access.

Our audit report was issued in September 1998 and recommended corrections to the noted INR deficiencies. To date we have not received a formal response from INR.

Unit Security Officers

Problems with the control of classified documents are not limited to INR. Many bureaus are not following security regulations for protecting classified information.

The Department requires the designation of an Unit Security Officer (USO) in each bureau and office. USOs are responsible for maintaining an active program to inform employees of their responsibilities for complying with security regulations. We found that USO responsibilities were not being performed because many USOs were not fully informed of their security responsibilities, and they did not believe they had the authority to enforce security procedures. The USO function was generally a secondary responsibility and supervisors were not emphasizing the security responsibilities of the USO.

USOs generally did not 1) institute security procedures such as a formal after-hours check system, 2) perform office security reviews, or 3) brief employees routinely on security regulations. In 21 of 23 offices inspected, there were no assurances that after-hours checks were performed or that classified documents were properly stored. Of 23 USOs interviewed, 17 did not perform office security reviews, only 5 of 23 offices escorted uncleared cleaning staff, and only 11 of 23 regularly briefed employees about security. We recommended that the Department increase the frequency of security briefings and related training afforded to employees and ensure that USOs receive periodic training.

We further recommended that the Department apply the model used for the Secretary's suite where a full-time, professional security officer was assigned to oversee and enforce adherence to security requirements and that DS assign security personnel to headquarters bureaus to augment the USOs, to perform as security advisors, and to oversee internal office security procedures.

In response, DS issued new security instructions. A formal USO training course is under development and is scheduled for implementation in 2000. DS also is working with bureau executive directors and personnel officers to require that USO evaluation reports include their USO responsibilities. OIG will verify when each of these measures is in place.

The Department has accepted our recommendation and is reviewing the feasibility of assigning an Information Security Specialist to serve in each bureau as the principal USO. However, DS has not received additional positions to meet this agreed upon program responsibility.

Security Incidents, Disciplinary Actions, and Investigative Referrals

OIG found an unacceptably low awareness and concern in the Department for the proper handling of classified material in part because awareness training and administrative actions taken to discourage the improper handling of classified material were not effective.

Security Incidents and Disciplinary Actions

The Department has a security incident program intended to identify improper security procedures and to educate employees in the proper safeguarding of classified information. An incident is defined as an infraction or violation, which is a failure to safeguard classified materials. A violation occurs when the failure to safeguard information could result in the actual or possible compromise of the material; an infraction occurs when the information was not properly safeguarded but does not result in the actual or possible compromise of the material. In 1998, the Department recorded 4 violations and 1,673 infractions.

The Department's contract guards perform inspections after regular working hours. Such inspections are fairly cursory, but several incidents of improper security are reported daily. When the Marine Security Guards visit the Department as part of their training, their inspections are much more rigorous. In 1998, inspections conducted by Marines at Main State resulted in an average of 63 infractions or violations identified during each of 8 inspections conducted. These incidents generally involved open safes and unsecured documents.

We also found that when INR distributed SCI material there were frequent instances where SCI was improperly handled, yet security incident reports were generally not issued. Rather, INR would attempt to retrieve the missing documents. In our view, when SCI material is not returned to an approved SCI facility at the close of business, an incident report should routinely be forwarded to DS for investigation. We recommended that INR implement procedures to ensure that SCI documents are returned to SCIFs each night.

The Department's security incident program has not been effective because security awareness and administrative and disciplinary actions have not been sufficient. Repeat offenders receive progressive levels of discipline. Repeat offenders receive letters of warning and, depending on the gravity of the situation, they can continue to retain their security clearances for access to classified information and retain their SCI access. We recommended that the Department increase the frequency of security briefings and related training, and the Department has begun to do so. We also recommended that the Department strengthen the disciplinary actions associated with security incidents. The Director General and DS are looking into options for implementing this recommendation.

Investigative Referrals

The Inspector General Act of 1978 (IG Act), as amended, and the Foreign Service Act of 1980, as amended, provide the OIG with a broad mandate to investigate fraud, waste, and abuse in the Department of State programs and operations. The OIG Office of Investigations is responsible for examining allegations of criminal activity and employee misconduct in Department programs and operations. This may involve wrongdoing on the part of an employee, contractor, or other individual doing business with the Department. Our jurisdiction encompasses violations of the criminal code such as visa and passport fraud, conflicts of interest, and false claims, as well as contract and procurement fraud and violations of employee standards of conduct, such as misuse of official position. The IG Act requires the Department to provide OIG with access to information and assistance during the course of an investigation. The Foreign Affairs Manual requires State Department employees to report to the OIG any information concerning fraud, waste, abuse, and mismanagement in Department programs and operations. In turn, my office is required pursuant to the IG Act to report expeditiously to the Department of Justice whenever we have reasonable grounds to believe there has been a violation of a Federal criminal law.

OIG Investigative Process

We receive allegations from a wide range of sources including other law enforcement agencies, Department managers, employees, and the general public. Each allegation is reviewed promptly and carefully. If the information provided to us is specific enough, we may open an investigation immediately upon receipt of an allegation. If the information presented is too vague, we open a preliminary inquiry in an attempt to develop more information or to clarify the information that has been provided. After a preliminary inquiry we will either open an investigation and assign an investigator or, if there is no information to substantiate the allegation, we will close the preliminary inquiry and take no further investigative action. If the circumstances warrant, we may refer the matter to the Department for its information or appropriate administrative action.

Section 603 of the Intelligence Authorization Act of 1990 (P.L. 101-193) requires information concerning violations of U.S. espionage laws by persons employed by or assigned to U.S. diplomatic missions abroad to be reported immediately to the FBI. Likewise, Section 811 of the Intelligence Authorization Act of 1995 (P.L. 103-359) requires us to advise the FBI of information indicating that classified information is being or may have been disclosed in an unauthorized manner to a foreign power. Accordingly, in these instances we would refer the matter to the FBI and provide appropriate assistance in the conduct of the investigation. The OIG has been actively involved in a limited number of counterintelligence investigations.

If there are allegations of other types of mishandling of classified information, we would refer the matter to DS for investigation and a damage assessment resulting from the mishandling of that information. If, however, the allegations involve aspects of employee misconduct we

would coordinate with DS to address the separate aspects of the case. Once an investigation is opened, agents will begin to gather the evidence and coordinate with the Department of Justice prosecutors to develop the case.

We conduct our investigations according to investigative procedures established by the Federal law enforcement community. This includes reviews of relevant files and documentation as well as interviews with and written statements from complainants, witnesses, technical experts, and subjects of investigations. Investigators use various law enforcement techniques, such as issuing Inspector General subpoenas duces tecum, consensually monitoring conversations, conducting surveillances, and executing search warrants.

Administrative Phase of an Investigation

When a criminal investigation is initiated, the Department may take some immediate administrative actions to safeguard the integrity of Department operations. For example, it may place the subject of the investigation on administrative leave, suspending the individual's security clearance or building pass, or temporarily detailing the individual to a non-sensitive position pending completion of the investigation. If a criminal investigation is declined for prosecution, it will typically be referred to the Department for administrative or disciplinary action ranging from admonishment or reprimand to suspension or removal.

****

Conclusion

In summary, Mr. Chairman, I am encouraged by the actions taken by Department management to correct the physical and procedural security deficiencies at Main State that we have noted in our work. Yet of equal if not greater importance is continuous vigilance by all Department personnel and an ongoing commitment to maintain and enforce the highest level of security awareness and compliance.

This concludes my prepared statement, and I am delighted to answer any questions that you may have regarding my statement.

TESTIMONY BY
J. STAPLETON ROY
ASSISTANT SECRETARY OF STATE FOR
INTELLIGENCE AND RESEARCH
MAY 11, 2000
HOUSE INTERNATIONAL RELATIONS COMMITTEE

Good Morning. I am glad to have the opportunity to appear before you today with my colleague, Assistant Secretary for Diplomatic Security David Carpenter, whom the Secretary of State has named as her senior adviser on security issues. We will be happy to discuss with you the Department's response to the disappearance of an INR laptop computer and other important security matters.

Let me begin by briefly reviewing the basic facts surrounding disappearance of the laptop computer. On January 31 a laptop computer containing highly classified information was discovered to be missing from a secure area controlled by the Bureau of Intelligence and Research at the Department of State, or INR, which I head. This matter is under active criminal investigation by the FBI and the Department's Bureau of Diplomatic Security, or DS. I have asked all personnel of INR to cooperate fully with the investigation. That is our sole role. We are not privy to the investigation's focus, time line and preliminary findings, so I cannot speak to those subjects.

In my testimony today, therefore, I will focus on four subjects: (1) INR's actions in response to the disappearance of the laptop computer; (2) the Secretary's decision to transfer formal responsibility for protection of Sensitive Compartmented Information (SCI) from INR to DS; (3) the resulting enhancement of the security regime within INR; and (4) the implications for INR's statutory role as a member of the Intelligence Community.

Disappearance of the Laptop

The laptop had been purchased in 1996 for the exclusive use of officers from other bureaus engaged in counterproliferation work who did not have access to classified work stations within INR. It was used and stored in an INR secure area because it contained highly classified information bearing on the proliferation of weapons and technologies of mass destruction and related delivery systems. Because of the sensitive information on it, the computer was not permitted to leave the INR secure area, where open storage was authorized under applicable regulations.

On January 31, INR staff could not locate the laptop in response to a request by a would-be user from outside the Bureau. When a careful search of the office suite failed to locate the laptop, the office in question took immediate steps to interview all personnel

in the office, as well as officers from outside the Bureau who had been authorized to use the laptop. Some of those approximately 40 officers were out of country on official business. They were queried by phone or cable. When these efforts failed to locate the laptop, INR's security branch chief launched a formal investigation and requested the office director to respond to a detailed list of questions. He also interviewed key individuals and developed a summary of relevant circumstances. When this internal investigative phase failed to locate the laptop, the INR security branch chief reported the circumstances to me along with his recommendation that because of the potential compromise of classified information, the matter be turned over to DS. I immediately approved this recommendation. On February 10, INR requested DS to commence an investigation and notified the CIA Center for Security that a computer presumed to contain sensitive classified material could not be located.

All matters relating to the investigation are under the purview of DS and the FBI, and I am not privy to the details. We do not yet know how the laptop disappeared from the INR secure area, whether it was removed by an employee authorized to work in the office, whether it was stolen for its material value, or whether it was taken for the information on its hard drive.

Regardless of the circumstances, the loss of the laptop is inexcusable. It should not have happened. As the Assistant Secretary for Intelligence and Research, I am also the Senior Officer of the Intelligence Community in INR, and in the Department of State. All personnel in INR, from top to bottom, have been indoctrinated and trained to be aware of their responsibility to safeguard the nation's most sensitive secrets. Whatever the results of the investigation, it is clear that we failed to exercise our responsibility to safeguard the computer and the classified information on it.

I particularly regret that Members of Congress first learned of the incident from the pages of the *Washington Post*. This was never our intention. That it happened is most unfortunate and is being looked into as part of our effort to draw lessons from this unfortunate experience.

The Secretary's Decisions in Response to the Loss

As a result of the circumstances I have just outlined, the Secretary took a number of steps affecting the Bureau that I head:

First, after consulting Director of Central Intelligence Tenet, the Secretary decided that DS should take over from INR the responsibility for protection of Sensitive Compartmented Information. I support this decision and am confident that DS will do the job well. We are working hand-in-glove with DS and with CIA to effect this transfer. In addition to improving security, I believe this will strengthen INR's ability to concentrate on what we do best, which is analysis and intelligence policy coordination.

In my view, this transfer of the SCI security function can be handled in a manner that will not conflict in any way with INR's responsibilities as a statutory member of the Intelligence Community. Indeed, since before the discovery that the laptop was missing, we had been working closely with DS to identify and formalize areas for enhanced cooperation.

Aside from the transfer of the SCI security function to DS, the Secretary also asked that in the investigation of the disappearance of the laptop, questions of accountability be examined carefully, and appropriate recommendations be made for decision. Meanwhile, to enhance confidence in the review process, two INR office directors have been temporarily transferred to other duties. This is not a finding of fault. It is to ensure that as the investigation is conducted and remedial steps are taken, there is full confidence in the process.

In addition, the Secretary directed that a number of other steps be taken to tighten security in the Department. Assistant Secretary Carpenter will be addressing these in his testimony.

The Security Environment within INR

The Secretary held a Town Meeting at the Department on May 4 to stress once more that all Department employees must attach the highest priority to their security responsibilities. I had already reinforced this message in a meeting with the entire INR staff on April 26, and I am confident that everyone in the Bureau is conscious of the need to maintain a high level of security awareness at all times and that security is an inextricable and indispensable part of all of our jobs.

Mr. Chairman, you inquired in your invitation letter to me about the day to day procedures for monitoring classified information within INR. In accordance with Director of Central Intelligence Directive (DCID) 1/19, Section 6.9, SCI security or control officers responsible for Sensitive Compartmented Information Facilities (SCIFs) maintain records, manual or electronic (bar codes), of external receipt and dispatch sufficient to investigate loss or compromises of SCI documents during transmittal.

Given the volume of classified and SCI material received daily in INR, we and DS have recognized the need to strengthen procedures for assuring document accountability. Earlier this year, we sought and gained approval to hire additional documents control specialists. Upon their entry on duty, they will work to ensure that both the theory and practice of document accountability within INR are fully in accord with intelligence community standards and requirements.

Following release of the OIG report last September, the DCI's Community Management Staff offered to make available to INR a professional document control specialist to evaluate our existing staffing and document control procedures, and to make appropriate recommendations. I understand the individual selected to assist us – expected

in INR very soon -- will come from the Defense Intelligence Agency, whose operational milieu is in important respects similar to that at State.

As regards the management of and security procedures for construction or renovation projects at Main State, in INR this relates primarily to projects that involve Sensitive Compartmented Information Facilities or SCIFs. Here "DCID 1/21 – Physical Security Standards for Sensitive Compartmented Information Facilities" is the governing directive. The DCID requires that whenever a project is contemplated, a construction plan, balancing threats and vulnerabilities, must be reviewed and approved by the cognizant security authority. In my view, these requirements are time tested and appropriate provided they are, as they should be, rigorously observed.

The INR Assistant Secretary's Role as Senior Official of the Intelligence Community (SOIC)

Mr. Chairman, you also asked in your letter of invitation that I focus on the security role of the Assistant Secretary for INR as the senior official of the intelligence community (SOIC), as distinct from the responsibilities now placed in DS. First, let me affirm that I see no statutory, regulatory or procedural barriers that need interfere with the ability of the Bureau of Diplomatic Security to carry out security responsibilities within INR. There are some fine points now being addressed, but these have not impeded in any way the transfer of day to day security responsibilities within INR to the Bureau of Diplomatic Security. Nor should this impede INR's ability to perform its functions as a member of the Intelligence Community.

As members of this Committee may be aware, the Department of State is not a member of the Intelligence Community; rather, it is INR within the Department, that is a statutory member. As Assistant Secretary of INR, I am the senior adviser to the Secretary of State on all intelligence matters and responsive to her direction. At the same time, I have certain responsibilities to the Director of Central Intelligence that derive from my status as the Senior Official of the Intelligence Community within INR. The authorities and responsibilities vested in SOICs are detailed in "DCID 1/19 – Security Policy for Sensitive Compartmented Information and Security Policy Manual." This directive states that intelligence organizations, as defined in E.O. 12333, have the authority and are responsible for all aspects of security program management with respect to the protection of intelligence sources and methods and for implementation of the DCIDs for activities under their purview. Hence, INR had previously maintained its own security program for intelligence sources and methods, while DS has developed and implemented security procedures, both domestically and abroad, for protection of the larger, more traditional universe of collateral classified information, physical and technical security countermeasures, VIP protection, etc. Pursuant to the Secretary's decision to transfer SCI security protection to DS, we are working with DS and CIA to develop the necessary procedures within the framework of this DCID.

Concluding Remarks

In conclusion, let me stress once again that the Department of State is undertaking a top-to-bottom review of security procedures. INR is a part of that process and, working closely with DS, we are moving simultaneously on many fronts to ensure better security throughout the bureau. As the Secretary said, a 99% grade on security is not a passing mark.

Thank you.

Statement of David G. Carpenter
Assistant Secretary of State for Diplomatic Security and
Senior Adviser to the Secretary of State on Security Issues
House International Relations Committee
May 11, 2000

Mr. Chairman and Members of the Committee, I am appearing before you today to answer your questions about the recent laptop incident. I am also prepared to discuss other domestic security issues affecting the Department of State.

I accepted the position of Assistant Secretary at the State Department with the full realization that the job would be challenging. But, I could never have envisioned the enormity of that challenge. I doubt that there are many outside the agency who appreciate the magnitude of the task thrust upon DS, the complexity of the issues faced in managing a global security program responsible for the protection of so many lives, and the challenges in facing off against sophisticated espionage services as well as transnational organizations focused on the destruction of American interests around the world.

On a positive note, I was extraordinarily gratified by the capabilities and professionalism of the people working in the Bureau of Diplomatic Security. They are clearly first rate. But I was shocked to learn just how much the State Department's budget had been cut and, to my regret, how hard those budget and personnel cuts had hit DS. I found that DS had people in all areas of its responsibilities who, in my experience, were second to none in other similar agencies but it became painfully obvious that DS, although talented and dedicated, had far too few people to meet the challenges it was about to encounter. Following the fall of the Soviet Union, DS was authorized to hire only a handful of agents, engineers, and civil service security personnel. Twenty percent of DS positions worldwide were reduced. The worldwide guard program was decreased by five percent. Rules and regulations concerning security were loosened to the point that holding employees accountable for serious security issues became more difficult. It is my assessment that the budget and personnel cuts had significantly eroded the Bureau's ability to fulfill even its most basic services. They had reached the point that when there were major conferences in the US, requiring significant manpower to staff protective details, numerous operational offices had to be shut down to support the effort. In some respects, this type of scenario still continues to this day.

Let me give you a few examples of how DS' programs were "streamlined" during that period. Among the activities affected was our Office of Counterintelligence. The number of positions was reduced from 41 to 26, and funding for the program was cut from $225,000 to $65,000. Staffing for programs in the Department that handle procedural and information security issues was reduced by more than fifty percent.

Our technical countermeasures programs suffered a similar fate as limited funding forced the Bureau to fund only priority life safety programs rather than invest in upgrading its antiquated countermeasures program. The Department's reaction to imposed fiscal constraints and a popular opinion that the cold war had ended and now the world was a better place had devastating consequences for DS programs.

In 1997, the Bureau's hiring picked up considerably, and while it appeared they were making strides in restaffing to the point of making it ready to meet its existing challenges, the bombings in East Africa occurred.

Let me say that those bombings have dramatically changed the magnitude and intensity of our overseas security programs and the support of this Committee in regard to our specific needs has been much appreciated.

As you are aware, nearly all of the new positions acquired since the bombings have been directed at overseas staffing or in support of our overseas operations, chiefly with antiterrorism in mind. The Department is currently reviewing staffing levels in other areas that may have been neglected including counterintelligence, dignitary protection, and domestic facility security which continue to be significantly understaffed and underfunded.

THE DS MISSION

Let me describe for you the universe of our efforts. We are in the protection business. We protect people, facilities, and classified information. And we do this at our posts throughout the world.

Let me give you some idea of the magnitude of our global life safety responsibilities. We protect approximately 10,000 State Department employees in the United States. Overseas, we are accountable for the protection of an estimated 75,000 US citizen employees and their families. Add to that number more than 37,000 foreign service employees working for our embassies and consulates. Each year we also protect approximately 130 distinguished high profile foreign visitors to the United States such as Yasser Arafat, the Dali Lama, and ministerial level

dignitaries. And that is an encapsulated view of just our mission to protect people.

Mr. Chairman, in my view, the breadth of this global mandate is unique in the federal government.

Our missions for protecting facilities and information are equally demanding. DS has designed programs to counter a global array of security challenges presented by elements ranging from common criminals to terrorists and spies. Our programs include safeguarding classified and national security information, personnel investigations, computer security and information security awareness programs, and the conduct and coordination of counterespionage and counterintelligence investigations.

In the past year much has been made of security incidents at Main State. Providing security for this building is a problem, not impossible, but still ver challenging.

The Department of State building is the second largest government building in the Nation's Capital. It is occupied by 8,500 employees and receives over 200,000 official visitors and tourists each year. The main State building covers two square blocks and has eight stories and a basement. There are 2.6 million square feet of space with 1.8 million square feet of occupied space. It has 5 pedestrian entrances, 3 basement entrances to a 900 plus vehicle garage, 2 loading docks, 43 elevators, 5400 windows, 9 acres of roof, and 13 emergency generators. The building has virtually no setback from the street thus affording little opportunity to screen either visitors or vehicles at appropriate distances.

The building serves as the hub for American diplomacy. It hosts numerous international conferences and major events involving world leaders each year. The building is the platform for the nation's daily press briefing on events around the world. It houses the nation's State Dining Rooms and an unrivalled collection of colonial and early Federal decorative "priceless" art objects insured for $100 million.

The Department has in place procedures and safeguards to protect our facilities during construction and renovation. As this Committee is aware, Main State is currently undergoing a major ten year renovation project. Security measures such as the development of construction security plans, construction surveillance, vetting of workers, screening of materials and other precautions are integrated into this project. Other construction projects performed within the building are routinely scrutinized by DS officers to determine the level of sensitivity and to ensure that proper security countermeasures are utilized.

In other words, the State Department building is a very large and busy institution. Protecting it is an immense challenge.

THE INCIDENTS

Three incidents in the Main State building have brought home to all of us the need to strengthen domestic information security. In February 1998 an unknown male in a tweed coat carried away classified documents from the Secretary's suite of offices. That case, which was investigated by the FBI, is in an inactive status at this time.

The second incident came to light on December 8, 1999, when Russian Intelligence Officer Stanislav Gusev was arrested on the street outside the State Department as he listened in on a meeting in the Department's Oceans and International Environmental Scientific Affairs' conference room via a bug planted in the chair railing. Gusev, who had diplomatic immunity preventing his prosecution in the US, was asked to leave the country. The investigation by the FBI continues into, among other things, how the bug was planted. Spinning off the bugging case was an inquiry into how a computer software contract was managed and whether the system on which the software was placed had been compromised. That inquiry is still underway.

The third incident is, of course, the laptop incident which is currently under investigation by the FBI and DS. Ambassador Roy has already described for you how the laptop was used, the circumstances surrounding its disappearance, INR's referral of the matter to DS, and the Secretary's five point response to the incident.

STEPS TAKEN

Mr. Chairman, we have learned some very valuable lessons from these incidents. The fundamental problem which has brought the Department to the point at which it now finds itself is not an absence of proper policies and procedures, as those are and have been in place. The problem is simple carelessness. That is, non compliance and/or disregard for established regulations. These incidents have prompted us to take measures which complement existing regulations and procedures and are designed to change the lax attitude toward security at the State Department.

I believe that substantial progress has been made over the past two years. We have tightened security in the Secretary's suite of offices. We have adopted a rigorous, comprehensive

escort policy, worked to strengthen computer safeguards, and assigned uniformed officers to floor specific patrols inside the building. At Main State we have an after hours inspection program of department offices. And we continue a program of bringing Marine Security Guards in training into the Department ten times a year to conduct security sweeps. We have closed D street outside the building to traffic and installed cement barriers around the entire building, thus lessening our physical vulnerability. Now, we have provided security awareness briefings to over four thousand department personnel. But, these are only the first steps. Much more needs to be done.

In March I convened an interagency review panel comprised of senior security representatives from the FBI, the Department of Defense, the US Secret Service, the CIA, and the Diplomatic Security Service. The panel was asked to review the countermeasures currently in place to protect against unauthorized access to the Main State Department Building and classified information. I also requested that they make recommendations to improve security at the Main State Building. On Monday of this week, I received the panel's report. I plan to present the report to the Secretary when she returns to Washington and intend to use it to correct systemic vulnerabilities at Main State. Once the Administration has had an opportunity to review the report, I will be delighted to share it with you, Mr. Chairman, and the Committee.

The panel confirmed our assessment of known weaknesses in our programs and recommended both short and long term solutions that it believes will enhance security at Main State. Their findings center on Main State's access controls, its physical security, information security, security awareness, our uniformed protective officer program, and the creation of a chemical/biological program. I am convinced that the development of a strategic plan to fund and implement these findings will result in significant improvement in our programs.

The Secretary's leadership in raising security awareness has been invaluable. She has personally emphasized security at every opportunity for the purpose of strengthening the culture of security at State. As you know, on May 3 she held a Department-wide town meeting on security because of the laptop incident. In the course of the meeting, she stressed that each of our employees must be "our neighbor's keeper" when it comes to security. The position that she has taken with respect to individual responsibility among our diplomats, that regardless how "skilled you may be as a diplomat … if you are not professional about security, you are a failure," has resonated throughout the Department. Further, when she told the Department employees that the press reports were accurate, and she was,

indeed, "furious" about our security lapses, any mistaken belief anyone might have had that the Secretary wanted simply to let this blow over and be forgotten was forcefully corrected.

I believe that what we have done and are doing, combined with the stark, ugly reality of what security failures produce, have gone a long way in raising awareness at the Department. I think that we have reached the point where the decided majority of State Department employees has recognized that a threat exists; that poor practices are unacceptable; that security is a high priority with the Secretary, this Administration, and this Congress; and that employees will be held accountable for lapses. I can assure you that the Secretary and I will continue to drive home those points as forcefully as possible.

As I said earlier, I believe that the lax attitude in the Department toward security is no longer tolerable. I fully expect that we will see that the Department's efforts aimed principally at better education at existing requirements and designation of individual responsibilities have borne fruit and that there will be substantial and voluntary adherence to security rules and procedures. But if I am wrong, we are fully prepared to use enhanced disciplinary procedures to further underscore the seriousness with which we view this issue.

Mr. Chairman and Members of the Committee, this concludes my statement, and I would be happy to answer any questions you have about the matters which have brought us here today.

WRITTEN TESTIMONY OF FEDERAL OF INVESTIGATION
SECTION CHIEF TIMOTHY D. BEREZNAY TO THE
HOUSE INTERNATIONAL RELATIONS COMMITTEE
MAY 11, 2000

Mr Chairman, Mr. Vice Chairman, and Members of the Committee, I am pleased to appear before you today to discuss State Department security issues of concern to this Committee. I will be as forthcoming as possible, given the sensitive and classified nature of aspects of the information requested by the Committee.

Concerning the missing State Department laptop computer, I want to ensure the Committee that the FBI's investigation of the missing computer is being afforded the highest FBI priority. As you are aware, I am prohibited from discussing the matter further as it is the subject of a pending criminal investigation.

The Committee has asked that I comment on the sufficiency of State Department security procedures in connection with the bugging of the 7th floor conference room by the Russian Foreign Intelligence Service. The FBI was asked by State Department in late August 1999, to conduct an environmental technical survey, in other words a review of neighboring properties to determine whether a hostile intelligence service might have acquired such property. This survey was specifically requested in connection with pending renovations at the Department. We were also pleased to have our Washington Field Office work with the Office of Diplomatic Security in 1998 to survey access to State Department by Russian intelligence officers. Beyond these narrow surveys, conducted with or at the request of State Department, the FBI was not called upon to review physical security procedures at the Department. Those matters were, however, addressed by the Office of the Inspector General in its September 1999, report.

The FBI believes the State Department acted swiftly during August 1999, to limit the number of unescorted foreign nationals visiting State Department following the discovery of the listening device in the seventh floor State Department conference room. On August 23, 1999, the State Department

implemented policy that requires all foreign nationals to be escorted within the building at all times. As noted by the Committee, there is an exception for foreign media correspondents issued unique but permanent badges that allow unescorted entry, without passing through metal detectors.

There is reportedly an understanding the media is not to go above the second floor, where the press office is located. This exception affords unescorted access to the State Department by a number of known foreign service intelligence officers. The FBI does not customarily provide other agencies, to include the State Department, with lists of intelligence officer identities, to protect both sensitive cases and sources, unless there is specific reason or if asked. If asked, the FBI would be willing to identify to the State Department permanent media badge holders identified as hostile intelligence officers so that their access could be restricted or their visits monitored.

Historically, hostile intelligence services have utilized media cover for intelligence activities in the United States. However, because intelligence officers under media cover do not have diplomatic immunity, they normally perform in-depth but overt intelligence collection. Clandestine handling of agents or other covert activity is usually assigned to intelligence officers under diplomatic cover. In addition to overt intelligence collection, intelligence officers under correspondent cover have been engaged in active measures campaigns designed to support their national interests and to influence United States policy makers. Active measures campaigns take the form of oral persuasions or the dissemination of written information favorable to their national policy--both of which are facilitated by intelligence officers under media cover. Hostile intelligence services use active measures as an inexpensive and relatively low-risk way to advance their international positions.

Over the last fifteen years, no foreign intelligence service officer under media cover has been declared persona non grata for engaging in espionage activities. This is attributed, as I previously noted, to the fact that these

officers are not accredited diplomatic immunity, and thus normally do not engage in clandestine agent-handling activities subject to interdiction.

With respect to your inquiry regarding the use of laptop computers, the FBI uses only specified laptop computers that carry appropriate safeguards for classified data, to include both use of passwords and encryption. These laptops are maintained by automation personnel and are available for short period loans to FBI employees. The laptop computers are periodically examined and the stored information purged; when they are turned in by one employee, and before being loaned to another individual, the hard drive is purged and reprogrammed. The laptop computers are also subjected to an audit and forensic checks to ensure they have not been compromised.

The FBI views the protection of classified information in a computer environment as a problem that is not unique to the State Department. It is a security issue that will continue to present problems to all members of the Intelligence Community.

Questions Posed for May 11, 2000, Testimony
House International Relations Committee

1. Has the State Department done everything it possibly can since the chair rail incident to minimize security problems and threats?

2. Does the gentlemen's agreement of no enforcement that badged foreign press officials should not have access to Main State without escorts pose a serious security threat?

3. The State Department's IG report of September 1999 cites the following "A recent FBI report stated that suspected foreign intelligence were granted unescorted access. The policy of unescorted access poses a significant security vulnerability etc etc." Has that problem been totally addressed at the State Department? Are there any foreign fellowship programs that result in foreign nationals being allowed in the State Department unescorted?

4. Shouldn't the State Department be vetting the foreign correspondents building access badge requests to ascertain if they are in fact intelligence officers of a foreign power before granting this privilege?

5. What is the Bureau's experience with foreign press officials using media positions as cover for espionage activities here in the USA?

6. What is the record of foreign press officials being declared persona non grata (PNG) over the last 15 years for engaging in forms of espionage using their media positions as cover?

7. How bad were State Department security procedures that allowed a Russian intelligence officer or its recruit to enter a seventh floor conference room at the State Department, and physically alter the structure of the room and implant a listening device?

8. How does the Bureau treat the use of lap tops for classified data? Is there use controlled and are user sign sheets mandated? Must they be pass worded?

Opening Statement of Hon. Chairman Benjamin A. Gilman
Status of Embassy Security Enhancements
Wednesday, May 17, 2000

Good morning. Today the Committee on International Relations is holding its second hearing on the recommendations of the Overseas Presence Advisory Panel. We will review the Panel's recommendation to create a new government corporation for overseas buildings, which would replace the Foreign Buildings Office in the State Department with an "Overseas Facilities Authority."

This new authority would be responsible for building, renovating, maintaining and managing the federal government's civilian overseas office and residential facilities. In their November, 1999 report, the Panel stressed that our overseas institutions are not equipped to operate effectively in the 21st Century.

They stated that our overseas presence is crippled by insecure and decrepit facilities, obsolete information technology, outdated human resources practices and outmoded management and fiscal tools.

The Panel concluded that an overhaul of the large property management program requires "more authority, more flexibility and increased participation by other U.S. government agencies with a significant overseas presence."

Presently the Foreign Buildings Office manages 12,000 properties in more than 250 locations. With the infusion of the emergency supplemental appropriations and current increases in appropriated funds for embassy security enhancements, the task for the Foreign Building Office has increased dramatically.

This hearing is an opportunity to discuss the proposal for a new corporation that would operate under different rules and procedures and presumably would have greater flexibility in financing and management practices. This Committee has heard from the Members of the Overseas Presence Advisory Panel and now will hear from the State Department on this proposal.

Additionally, this Committee has been closely following the progress of enhancing the security of our overseas posts, including buying land and initiating new construction.

We appreciate the staff-level briefings that have been provided since the emergency supplemental funds were provided, and look forward to hearing from the Department on the current standing of the facility enhancement plan.

Admittedly, the State Department has a tough job of quickly trying to harden the security vulnerabilities of overseas posts, while also making sure that taxpayers' dollars are being wisely spent. Recognizing this fact, the Overseas Presence Advisory Panel proposed recommendations to leverage the overseas building program, which we will explore today.

Foremost, there should be no compromise when it comes to protecting our embassy employees and ensuring a safe physical environment.

The Overseas Presence Advisory Panel accurately captures the security situation at the State Department by emphasizing an integrated approach to security and developing a ***culture of security***.

Establishing this "security mindset," as they called it, will make the job before you, as the executers of the physical security program, infinitely easier.

Now, we welcome our panel of Administration witnesses to discuss the overseas building program and related security matters.

This morning I would first like to introduce Mr. Patrick Kennedy, Assistant Secretary for Administration at the State Department. Mr. Kennedy has been with the Foreign Service for 27 years and probably holds the record for the longest service as Assistant Secretary for Administration. He deserves a tribute for his outstanding service to the Department and to this Committee.

We again welcome Mr. David Carpenter, Assistant Secretary for Diplomatic Security, who appeared at our hearing on State Department security last Thursday. Mr. Carpenter assumed the position of Assistant Secretary in August of 1998, following a 26-year career in the U.S. Secret Service. He is the first person to hold this post who has a professional background in the protection and security fields. He assumed this responsibility at a critical time for all elements of security.

Finally, we are happy to hear again from the Inspector General of the Department of State and the Arms Control and Disarmament Agency, Jacquelyn Williams-Bridgers.

Ms. Williams-Bridgers was sworn in as Inspector General in 1995. She has been before this Committee many times and we appreciate the valuable work of her good offices.

The Honorable
Doug Bereuter

HIRC Hearing on Embassy Security
May 17, 2000

Mr. Chairman, the Crowe report on Embassy security highlighted the threat posed to our Embassies overseas from large vehicular bombs. Experience has shown in recent years that they represent the greatest physical threat to the lives and welfare of our employees and citizens. Over 80% of our overseas missions lack the adequate 100 foot setback to protect against such attacks. Although the Department has tried hard to correct many of the vulnerabilities cited in the Crowe report and elsewhere, until the threat from vehicular bombs is addressed, these efforts will be insufficient to deal with the primary threat. The Accountability Review Board, the OPAP report and numerous senior Department of State officials responsible for security have publicly come to this same conclusion.

The fact of the matter is that there is no substitute for purchasing, constructing or leasing property and new facilities that give us the necessary setback. Unfortunately it is also true that the Department and the Office of Foreign Buildings (FBO), for a whole variety of reasons described in the OPAP report and elsewhere, are not currently able to address this problem in a timely manner. It often takes literally decades to go through the labyrinth of bureaucracy associated with constructing a new embassy. The addition to Embassy Moscow took almost two decades. The State Department has been considering additions to the terribly outdated Beijing Embassy for a decade and construction has yet to begin.

In part, the problem stems from the scoring rules imposed by OMB that require all the costs of construction or lease purchase be scored in the first year. This makes it extremely difficult to get the necessary appropriations. It also costs the taxpayers millions and millions of dollars by causing the Department to rely on short term lease arrangements, which are far more expensive than either lease purchase or construction. For decades, the Department has been pouring money into short term lease payments for substandard, unsecure facilities when it could have been buying and constructing quality secure facilities at lower costs. Last year I offered am amendment to H.R. 2415 that would permit budgetary scoring of leased properties on an annual basis. Unfortunately, the amendment was ruled out of order. OMB has consistently rejected requests by government agencies for exceptions to the scoring rules.

The OPAP report endorsed the Crowe panel recommendations and proposed an innovative approach towards dealing with the problem and managing U.S. Government property

overseas by establishing a performance based public/private corporation (the Overseas Facility Authority, OFA), to replace FBO. It is my understanding that public/private corporations can be exempted from OMB scoring rules. The OPAP report notes that "in order to undertake the sort of fundamental change in the funding and management of U.S. Government overseas assets, FBO should be replaced by an OFA with more authority, more flexibility, and increased participation by other U.S. Government agencies." The OPAP report makes a compelling case for why a public corporation would be a more efficient and effective way of managing U.S. government facilities overseas and of dealing with the urgent issue of making these facilities more secure. Yet the Department appears to have rejected this idea. Why?

There would be many advantages to proceeding with the OPAP recommendation to replace FBO.with a government chartered public/private corporation. One of these is that we will have secure Embassies years earlier than would otherwise be the case and the security of U.S. personnel overseas would be dramatically improved as a result. I hope the State Department will look again at the excellent recommendations made by the OPAP panel in its report and the Staff study annex on capital improvements and will move expeditiously toward implementing these recommendations.

PREPARED STATEMENT OF PATRICK F. KENNEDY, ASSISTANT SECRETARY OF STATE FOR ADMINISTRATION, BEFORE THE COMMITTEE ON INTERNATIONAL RELATIONS, U.S. HOUSE OF REPRESENTATIVES, MAY 17, 2000

Mr. Chairman: I appreciate the opportunity to appear before your Committee. It is always a pleasure for me to be able to update you on the many accomplishments that the Department has made in improving our overseas security posture, facility infrastructure, and our worldwide facility operations. Obviously, since the tragic bombings of our embassies in East Africa, the issues concerning our infrastructure and the security of our missions overseas have received great attention within the Administration and the Congress. We very much appreciate the support of the Congress, and particularly of this Committee, for the Emergency Security Supplemental and the Administration's proposals for physical security upgrades at our overseas posts. I would also like to say a few words today on the Overseas Presence Advisory Panel (OPAP) and its recommendations concerning our Office of Foreign Buildings Operations (A/FBO). Finally, I will give a brief report on what we are doing at the Main State headquarters building here in Washington and the issue of security clearances for custodial and operations and maintenance personnel.

As you know, the Overseas Presence Advisory Panel, which issued its report last November, described many of our facilities abroad as unacceptable in terms of security and condition. Fully 85 percent of our facilities do not meet optimum security standards. Some are in need of extensive renovation. Some are seriously overcrowded. Most, however, simply have to be replaced. To protect our employees overseas, our goal is to expeditiously locate into safe facilities more than 22,000 embassy staff in over 220 vulnerable buildings. This is a formidable task. Achievement of this task will require an enormous initial and sustained level of capital investment. Mr. Chairman, quite frankly, during the past 10 years, we neither requested nor received sufficient funding to allow us to maintain our infrastructure base. Most recently, since the 1998 bombings, we are finally beginning to arrest that decline in resources, thanks to the support of the President and the Congress, and have taken the first steps toward rebuilding our facilities infrastructure. In fiscal year 1999 alone, A/FBO obligated over $800 million, the most ever obligated in a fiscal year, to replace unsafe facilities and improve security at those posts whose facilities cannot be replaced for several years.

As part of OPAP's overall charter to evaluate the way the United States organizes its overseas activities, it made 44 recommendations in eight general areas. This morning, I would like to focus some of my remarks on the Panel's recommendation to establish an Overseas Facilities Authority (OFA).

The Panel advocated replacing the Bureau of Administration's Office of Foreign Buildings Operations with a federally chartered government corporation—an Overseas Facilities Authority. The issues that led to the Panel's proposal included the perception that A/FBO-managed construction projects took longer and cost more than comparable private sector projects, that timelines were not always met, and that staffing levels appeared to be too high for the number of properties and projects being handled. However, I believe that the staff work that underpins these perceptions is faulty, as it failed to give due consideration to security requirements and special overseas needs.

The Panel proposed creating a government-chartered corporation that would allow the use of management and financing techniques commonly found in the private sector. This new authority—OFA—would exercise responsibility for building, renovating, maintaining, and managing the Federal Government's civilian overseas facilities, including office and residential facilities. As envisaged by OPAP, the OFA, in addition to receiving annual appropriations from Congress, would have features not currently available to the Office of Foreign Buildings Operations, including receiving funds from other agencies, levying capital charges for new facilities, obtaining forward funding commitments from the Federal Budget and loans from the U.S. Treasury, as well as retaining service fees from sources approved by the Congress. The OFA, again, unlike the current A/FBO, would have the ability to apply management techniques commonly used in the private sector to include using financial incentives and performance-based compensation standards. The Panel reasoned that higher salaries and incentives would allow OFA to attract highly qualified real estate and other professionals and further motivate employees and contractors to better meet construction project schedules.

We are currently giving serious and careful consideration to the Panel's proposals to reinvent the method of funding and administration of our overseas facilities' design and construction program. An interagency group headed by the Director of the Office of Foreign Buildings Operations, Patsy Thomasson, is reviewing all aspects of overseas facilities. Earlier this year, Ms. Thomasson formed six teams within A/

FBO to look in to, and analyze in depth, five critical areas—organizational structure, financing alternatives, business process reengineering, customer focus, and communications. A sixth team manages the overall effort. Together, these teams will make recommendations on how the Panel's desired outcomes can best be achieved. We have also contracted with a leading consulting firm to examine various funding options and ways to make A/FBO a more performance-based organization. While these team efforts are still continuing, I believe that creating an independent OFA is not essential to accomplish the changes that OPAP laid out. Most of the proposed attributes of the OFA could be assigned either administratively or legislatively to A/FBO without disrupting and halting the very positive direction in which A/FBO is now headed.

Although we agree with the thrust of the Panel's recommendations, we question whether the creation of an independent, federally chartered organization, comprised of both the public and private sectors, is necessarily the best approach to meet our infrastructure challenges overseas. Principally, we are concerned that such an entity may compromise the vital link between foreign policy and facility decisions. For example, there are foreign policy issues, such as reciprocity, that are intricately intertwined with overseas facility programs. Such is the case with China, where we are seeking a site for a new embassy in Beijing and China is seeking, as a condition, a site in Washington. Such is also the case with the United Arab Emirates, where we are seeking to acquire a parcel of land adjacent to our embassy in Abu Dhabi, and they want a new residence for their Ambassador here in Washington. These are classic examples where facility decisions are affected and sometimes driven by foreign policy considerations.

The Panel also urged that we continue to implement the Accountability Review Board's (ARB) proposals providing for security upgrades at our overseas posts throughout the world. We are doing that, and I am pleased to report that the Office of Foreign Buildings Operations has been particularly successful in responding to the mandates of the security supplemental that followed the 1998 bombings. Interim facilities are fully operational in Dar es Salaam and Nairobi, and we are moving smartly toward constructing permanent facilities in both locations. The Office of Foreign Buildings Operations conducted a competition for a fast-track design/build contract and awarded the contract last September. The designs of these projects have now reached the point where we anticipate giving the contractor the green light to mobilize onsite at Dar and Nairobi next month. We have also opened a temporary office building in Doha and are fitting out three buildings in Pristina to serve as temporary facilities. We have permanent facilities under construction in Doha and Kampala.

Currently we have 14 new embassies or consulates in various stages of development: Dar es Salaam, Nairobi, Abu Dhabi, Abuja, Berlin, Doha, Istanbul, Kampala, Luanda, Rio de Janeiro, Sao Paulo, Seoul, Tunis, and Zagreb. We are also in the process of acquiring several additional new office building sites. Also, since the bombings, A/FBO has completed 15 major rehabilitation projects at overseas posts with another 46 major rehab projects ongoing at this time.

Since the bombings we have also relocated many overseas Department and other Agency personnel to more secure facilities. For example, AID personnel have been/are being relocated to more secure facilities in Almaty, Antananarivo, Asuncion, Ashgabat, Cairo, Kampala, Luanda, Manila, New Delhi, Rabat, Tel Aviv and other locations around the world.

Increasing setback from streets and other buildings is another way of reducing the threat to loss of life and injury. During the past year and a half A/FBO has been extremely active in acquiring 87 setback properties at 25 posts around the world to provide greater security to our personnel. Negotiations and investigations are continuing on another 31 properties at 14 posts.

Worldwide Security Upgrade funding appropriated by the Congress has enabled A/FBO to approve 1,051 security upgrade projects at overseas posts with 34 percent of these projects having been completed. Every project will further protect our employees overseas. The Worldwide Security Upgrade Program which includes security projects such as the installation of berms, bollards, and access controls, is being executed at each post by A/FBO, the post itself, and/or by an implementation contractor or basic ordering agreement contractor. Other components of this program include the installation of shatter resistant window film on all office windows and the installation of forced entry/ballistic resistant (FE/BR) doors and windows. The bombings in Africa demonstrated all too tragically that the greatest threat to life and injury from a bomb blast is from flying shards of glass. Since the bombings, we have purchased 5.5 million square feet of window film. Nearly half has been installed, with the remainder to be installed by the end of the summer. We have also installed or replaced over 500 FE/BR doors and windows.

A/FBO's Asset Management Program, which acquires essential property by using proceeds from the sales of excess or underutilized properties, has been very successful, purchasing 18 properties in fiscal year 1999 and the first half of FY2000, while disposing of 17 properties.

These successes are the result of retorquing internal processes, applying new initiatives, and introducing innovative methodologies. These have all been key factors in achieving A/FBO's high level of productivity over the past 18 months. Today's Office of Foreign Buildings Operations is not the A/FBO of the late 80's and early 90's under the Inman program.

A 1991 General Accounting Office review of the management of the Security Construction Program revealed problems that A/FBO experienced during its efforts to meet the major challenges of the Inman buildup a decade ago. The most significant difficulties were linked to inadequate staffing, difficulties with overseas site acquisition, contractor performance, and the lack of an effective strategic focus. Since those years, however, A/FBO has implemented lessons learned throughout the organization and is now well prepared to undertake a large construction program.

A/FBO has developed an improved strategy for effectively executing a difficult, expanded construction program and has augmented its staff to handle the workload. The strategy is derived from A/FBO's Inman experience with the simultaneous execution of large, multi-year projects, and from implementing construction industry best practices. Included in our strategy are a number of initiatives described below.

• Design/build contracting. A/FBO is placing greater reliance on design/build (D/B) contracting. This method has been demonstrated in both the public and private sectors to reduce cost and save time in project delivery as compared with the more traditional two-contract, design-bid-build procurement method. In addition, we are looking at other multiple projects that could be packaged into groups for award to a single, large D/B contractor, as we did with the Dar es Salaam and Nairobi projects. Additional D/B contracts could be awarded for groups of projects in the out years.

D/B contracts are being managed by integrated project management teams to provide effective controls and added expertise. From the start of a project, these cross-discipline teams are accelerating project execution; controlling costs; clarifying lines of authority; and carefully defining roles, responsibilities, procedures, project priorities, and milestones. Potential risks to project success are identified and mitigated early.

• Staffing. A/FBO is much better positioned than in the mid 1980's when the Inman program began, and its in-house work force numbered less than 200. The professionalism and depth of the work force has increased as its size has grown to over 760 today. Eighty-four new staff members have been, or are being, brought on for worldwide security upgrades alone. Additional real estate professionals have been hired to find and acquire new sites and buildings; more design, engineering, project management, and other professionals and specialists have been brought on to execute construction projects. Overall, since the bombings, A/FBO has increased on board staffing by 17 percent.

Contract support has been increased, with Perini Corporation and Brown and Root assisting with security upgrade work, and with indefinite quantity contractors increasing A/FBO capabilities, especially in design-review services.

• Priority setting. The Accountability Review Boards recommended spending $14 billion on embassy construction in the next 10 years to replace all facilities that do not meet standards. Interagency Embassy Security Assessment Teams (ESATs) determined that most of our posts have compelling facility needs, such as for adequate setback, structural hardening, relocations, and other security requirements.

All chanceries, consulates, and multi-tenant annex buildings have been evaluated for security vulnerability. The analysis assessed the soundness of each building's structure and facade, the adequacy of the building compound's perimeter security, the building's setback from adjacent property, the post's political violence security threat, and additional security considerations that included the capability and willingness of the host country to control its internal and border security relative to external terrorists; as well as other factors. The resulting ranking was reviewed by stakeholders, i.e., regional bureaus, other agencies, the Bureau of Diplomatic Security, Embassy Security Assessment Teams, and A/FBO managers. Projects were then planned for different fiscal years based on vulnerability, stakeholder input, and consideration of factors that will either inhibit or facilitate a project's execution.

• Other measures developed or enhanced since the 1998 bombings. Time and space preclude a full explanation of all the other industry best practices adopted by A/FBO, however, a representative listing of these best practices follows:

- Industry Outreach
- Enhanced Partnering

- Security and Blast Research
- Site Search Program
- Pre-qualified A/E Pool
- Generic Statement of Work
- A&E Design Guidelines
- Integrated Building Systems
- Information Technology
- Signage Program
- Standard Delivery Process
- Site Adapted Office Building
- Project Execution Support Contractors
- Reliability Centered Maintenance
- Serviceability Tools and Methods
- Post Occupancy Evaluation

These "best practices" or initiatives, added to intense efforts by the Department, have resulted in the outstanding record of achievement over the past 18 months, and clearly demonstrate that today's A/FBO has the ability to manage a large and complex building program.

Let me turn now to the Department's buildings and facilities in Washington and elsewhere in the United States and the issue of security clearances for custodial and operations and maintenance personnel.

The Department of State occupies 58 buildings located throughout the United States, totaling approximately 6 million square feet of space. The Main State building in Washington, the domestic building you are most interested in, comprises roughly 2.5 million gross square feet and houses more than 8,000 employees. Given that size and population, Main State is similar to a small city in the services that are required. As you can imagine services to such a large population must include electrical, heating, air conditioning, plumbing, painting, carpeting, furniture, communications, custodial services, and all other normal maintenance and repair specialties employed on a daily basis. There are two major contracts that supply the majority of services in Main State, custodial and operations and maintenance (O&M). Those contracts are competitively bid and the contractors have corporate clearances at the appropriate level for their work; the custodial contractor has a corporate top secret clearance while the maintenance contractor has a corporate secret clearance.

In addition each contractor has employees who are cleared at the appropriate level in order to perform their jobs within the building. For example, the custodial contractor has 20 custodial workers with top secret clearance to work in sensitive and classified areas. Ten more have top secret security clearances pending. If a maintenance or custodial worker must work in a classified area and the worker has no clearance, that person is escorted by cleared Department of State personnel. Furthermore, it is the responsibility of the occupant of any space classified or not, to watch over custodial and maintenance workers in their area and protect all material for which they are responsible.

The Department is currently undergoing extensive renovations to bring the building up to par. The overall Main State renovation project, primarily funded by GSA is a multi-million dollar project. That work, which is in its early stages, is being done with GSA contractors. GSA's contractors have corporate clearances as well. In addition, with the Congressionally mandated reorganization of the Foreign Affairs agencies, State is in the process of absorbing the former USIA and ACDA staffs and functions. This has led to further renovation and construction work in the Main State building at a cost that will exceed $80 million and will involve probably 200 smaller construction projects, utilizing perhaps as many as 12 different contractors. Those contractors will all have corporate security clearances and most of the workers will also have clearances. The Bureau of Diplomatic Security (DS) is involved in those projects as well. DS is a member of each project team in this process and we work closely together to ensure that security requirements are met.

I would be pleased to answer any questions.

David G. Carpenter
Assistant Secretary of State for Diplomatic Security
Before the
House of Representatives
Committee on International Relations
May 17, 2000

Good morning, Mr. Chairman and members of the Committee. I welcome this opportunity to testify before you on the security profile of our United States facilities overseas.

On August 7, 1998, our embassies in Dar es Salaam, Tanzania, and Nairobi, Kenya, were bombed simultaneously by extremists bent on the destruction of American presence throughout the world. These tragedies unleashed a massive and intense effort to provide much needed security improvements at all our overseas posts. Although much has been accomplished, more needs to be done. Our overseas facilities are generally more secure now than in August of 1998, but the continuing threat environment worldwide requires that we not lose focus, that we continue to explore new ways of protecting ourselves, and support a program for new embassy construction.

The Department has aggressively upgraded security at previously low and medium threat posts to standards that were formerly only applied at high or critical level embassies or consulates. High and critical level posts have also received significant upgrades of equipment to better fortify their facilities. We no longer believe, in an era of transnational terrorism, that we have low or medium threat posts, nor do we believe that we will receive tactical intelligence of an imminent attack. Simply put, we must be prepared for any eventuality that presents itself.

Our goal following the bombings was to immediately improve the security of our threatened consulates and embassies, and we have done so. But at the outset let me say that it is important for this Committee to know that we still have a very basic problem that cannot be fixed quickly. The vast majority of our diplomatic posts fail to meet one of our most basic security standards, namely, the 100 foot setback standard. Until we can build embassies meeting the setback and other security standards, our efforts cannot provide the degree of security all of us want for our people and facilities.

STEPS TAKEN

Having recognized that we still have grave security concerns overseas, it is also important for the Committee to know that we have done a lot and that our embassies and consulates are more secure now than ever before. In this regard, let me review for you what we have done through our security upgrade program. Some of these actions have been based solely on DS initiatives; others were suggested by the Accountability Review Boards chaired by Retired Admiral William J. Crowe, the report of the Overseas Presence Advisory Panel (OPAP), and the Office of the Inspector General.

As previously stated, we are aggressively upgrading security at low and medium threat level posts to standards that previously only applied to high and critical rated posts. We have put in place physical security upgrades at our embassies and consulates such as reinforced perimeter walls, bollards, guard booths, vehicle barriers, and shatter resistant window film. We are upgrading and deploying security equipment to include better lighting, cameras, and video recorders; bomb detection equipment; armored vehicles, alarm and public address systems; and x-ray equipment. Where possible, we have mitigated the lack of sufficient setback by closing streets and provided for mandatory vehicle inspections.

We have also expanded our Anti-Terrorism Assistance training to aid foreign police in combating terrorism through appropriate programs as surveillance detection, border security, explosive detection, crisis management, and maritime security.

In addition, we have installed alarm systems at embassies and consulates to alert personnel to impending emergency situations and have instituted a program for the employees to "duck and cover" when the alarms are sounded.

We have also created a new security environment threat list with a modified methodology and criteria for determining threat levels. This process now addresses transnational terrorism as a distinct category as well as the threats from indigenous terrorism and political violence, and the threats from intelligence services, both technical and human, and, of course, crime.

DS has also changed the focus in training courses for Regional Security Officers and Special Agents to give them greater training on counter-terrorism methodology; explosive

ordnance recognition and disposal; chemical/biological weapons threats and defenses; and surveillance detection techniques.

In response to a specific recommendation from the Accountability Review Boards chaired by Retired Admiral William J. Crowe, we are also working with the FBI to better analyze law enforcement information which might have a bearing on threats to our missions overseas and to more quickly disseminate that information to appropriate posts. To that end, a DS special agent has been detailed to the International Terrorism Section at FBI Headquarters, and DS special agents are participating in the FBI's Terrorism Task Force.

DS has also established the office of The Coordinator for Chemical Biological Countermeasures. That office, which is conducting a worldwide survey to determine vulnerabilities, has purchased and is distributing Chemical Biological equipment to all posts. As part of its educational program, it has distributed instructional materials, including a pamphlet, videos, and a series of cables, to alert all posts to the nature of the threat and to provide defensive guidance. It has also established a comprehensive training program for security professionals and first responders.

The newest addition to our programs and of major significance has been the establishment, in less than one year, of surveillance detection programs at almost all of our overseas posts. A critical lesson learned from the bombings is that there is intense surveillance conducted against our facilities prior to an attack. Since going operational in January 1999, surveillance detection teams, most of which work with host government's security services, have observed over 700 suspected incidents of surveillance against our personnel and facilities. It has, in a sense, expanded our security perimeter and zone of control beyond our previous limitations. The surveillance detection program is clearly a "work in progress," but we feel that it is destined to become a major aspect of our overseas security defenses.

Finally, and I believe most importantly, DS has hired 234 new special agents and 17 security engineering specialists which has allowed for the creation of 140 new Security Officer positions abroad. By the end of Fiscal Year 2000, we will have 420 DS special agents serving as security officers in 157 countries. DS has also hired 20 additional diplomatic couriers, 34 maintenance technicians, and 46 civil servants in support of overseas security.

This is National Police week. On Monday on the very grounds of this capitol we paid tribute to this country's law enforcement heroes who gave their lives in the line of duty in the past year. Over the years Diplomatic Security has had its own heroes, some who gave their lives and others who lived to continue the fight. I am positive that out of this new cadre of special agents and other security specialists we will have more heroes. I thank this Committee for its support in hiring these new people and hope that I can look to you for support as we seek additional positions to strengthen our programs. It is people that will make the difference; that is, trained, motivated and dedicated professionals with the single purpose of insuring the safety of our overseas personnel and facilities.

REPLACING FBO, REGIONALIZATION, AND POST CLOSINGS

Mr. Chairman, with regard to your request for my views regarding the creation of a new agency to replace FBO, let me assure you that we have enjoyed a positive and close working relationship with FBO as is necessary to support our diplomatic personnel, to improve security, and to upgrade our facilities worldwide. We have a construction security management group working within FBO that helps to strengthen this partnership. I do not believe that distancing DS from FBO would enhance our security effort. Furthermore, I personally do not see how an independent entity would be more capable of overcoming the challenges and obstacles that FBO currently faces.

You have also asked for my views on the OPAP proposal to make greater use of regionalization as a means to reduce the number of personnel needed at posts and for my views on whether any posts will be downsized or closed because of security threats.

OPAP recommended creating a process "to right-size our overseas presence, reduce the size of some posts, close others, reallocate staff and resources, and establish new posts where needed." State and other agencies formed an interagency committee to review how to implement the right-sizing recommendation in the OPAP report. In early March, a pilot program began at a number of posts for the purpose of developing recommendations for right-sizing at these posts and to develop criteria that can be applied universally. What I have seen thus far, Mr. Chairman, suggests that regionalization efforts could result in reducing the size of some posts, but would inevitably result in increasing the size of others. But from a security

standpoint, I doubt that there would be any measurable savings in such an effort. My concerns are primarily focused on decisions related to where the regional posts are to be located and assurance that the prescribed security standards are in place. Certain countries present particularly difficult environments in which to work. By that I mean, high crime, inadequate infrastructure, unstable government, poor police support, and so on. Yet they may provide a geographical advantage as they are centrally located hubs for air transportation or viewed as a gateway to the continent. Believing that security is an important factor when entertaining ideas of regionalization, it is critical that no decision be made without proper vetting of life safety issues relative to these regionalization issues.

SUMMATION

Mr. Chairman, this concludes my testimony. As I indicated at the beginning, we have been diligent in our efforts to upgrade security at our overseas posts, and we have been successful in making those facilities safer now than they have ever been before. Nevertheless, there is still much that needs to be done, and until all of our facilities meet the basic security requirements, none of us will be satisfied with our security posture overseas.

I appreciate the interest you and the Committee have taken in this topic and will be happy to answer any questions you may have.

STATEMENT OF
JACQUELYN L. WILLIAMS-BRIDGERS
INSPECTOR GENERAL OF THE
U.S. DEPARTMENT OF STATE AND THE
BROADCASTING BOARD OF GOVERNORS

FOR THE
HOUSE COMMITTEE ON INTERNATIONAL RELATIONS

MAY 17, 2000

Mr. Chairman and Members of the Committee:

Thank you for the opportunity to testify before the Committee on the Department of State's efforts to correct security vulnerabilities at 101 domestic facilities and 260 diplomatic and consular posts around the world. As demonstrated by the terrorist attacks on U.S. embassies in Nairobi and Dar es Salaam in August 1998, perhaps no greater challenge exists for the Department than providing adequate security to protect our people, facilities, and information.

On October 5, 1998, Admiral William J. Crowe chaired an Accountability Review Board (ARB) to review the circumstances of each of the bombings, to assess the adequacy of our security systems and procedures, and to recommend improvements to them.

Among its many findings and observations, the ARB Report concluded that the Department does not apply its security standards fully. For example, neither the chancery in Nairobi nor the chancery in Dar es Salaam met the Department's standard for a 100-foot (30- meter) setback zone. Both were "existing office buildings" occupied before this standard was adopted, therefore, a general exception was made. As indicated by the ARB, "such exceptions worldwide with respect to setback and other non-feasible security standards reflects the reality of not having adequate funds to replace all sub-standard buildings within a short period of time."

The Congress appropriated $1.5 billion in an Emergency Security Supplemental Appropriation in fiscal year 1999 (FY 1999). Of that amount, $627 million was for facility security upgrades under the Security and Maintenance of U.S. Missions account, including about $163 million to stand up our operations in Nairobi and Dar es Salaam. Most of the remainder of the $1.5 billion was dedicated to upgrading existing facilities around the world, hiring extra security officers, and providing crucial anti-terrorism training for foreign government police forces. In FY 2000 the Department requested and received an additional $300 million to continue building secure facilities and $254 million for continuation of technical and perimeter security improvements. The Department of State has requested over $1 billion in FY 2001 for worldwide security upgrades, of which about half is for new buildings.

In November 1999, the Overseas Presence Advisory Panel (OPAP) completed its work on recommended reforms to improve the infrastructure of our overseas platform. The Panel's work leading to these recommendations was made possible by the tremendous commitment of government and private sector leaders, who brought to their undertaking their diverse experience in diplomacy, business, the military, and public interest groups. In

The Report of the Overseas Presence Advisory Panel, the Panel concluded that the "overseas activities of our government are critical to the advancement of the nation's interests and that the way the U.S. Government conducts these activities needs significant improvement if the strategic goals of U.S. foreign policy are to be achieved."

As you requested in your letter of May 11, 2000,1 will review with you today the work done by the Office of Inspector General including our findings and recommendations on the embassy security enhancement program and the use of the Emergency Security Appropriation. I also will discuss the Department's compliance with overseas security standards and other security challenges. Many of the recommendations stated in the Accountability Review Board Report and the Overseas Presence Advisory Panel report echo the recommendations that OIG has issued in recent years based on our audits and inspections of overseas posts.

In my testimony I will address these issues within the context of:
The OIG's unique security oversight role,
Securing our overseas missions,
Information security, and
Funding and managing future capital investments.

OIG'S SECURITY OVERSIGHT

State OIG is unique among Inspectors General (IG) in that in addition to audit, inspection, and investigation, we also conduct security oversight inspections of all U. S. Government facilities overseas (except those under our regional military commanders).

Since the bombings of the embassies in Nairobi and Dar es Salaam, the protection of our people, information, and facilities has become an even more critical mission for the OIG. I have created multidisciplinary teams in OIG to evaluate the implementation of many physical security initiatives and to monitor the expenditure of $1.5 billion in the emergency security appropriation. As part of our regular, on-going review of embassies, by the end of fiscal year 1999, OIG had evaluated the physical security and emergency preparedness of 42 embassies since the bombings. In addition, we are now completing the final in a 6-year series of reviews of the new Secure Chancery Facility in Moscow which had its official opening on Friday.

SECURING OUR OVERSEAS MISSIONS

The most significant security challenge for the Department is the protection of its overseas employees' lives while at work and at their residences. From a physical security standpoint this means upgrading the perimeter security of buildings, especially chanceries; building new chanceries to replace those that are clearly unsafe; and co-locating all agencies into protected areas. The second security challenge is the protection of classified and sensitive material, increasingly electronic information, both on the domestic front and overseas.

It is clear from recent events that all our overseas missions are at risk. The Department has made great strides to enhance the physical security of our overseas missions, and today, U.S. missions are more secure than they were 18 months ago.

Immediately after the East Africa bombings, the Bureau of Diplomatic Security mobilized its of fibers to survey our missions around the globe to determine which posts were most at risk from the new, transnational terrorist threat. The Department identified 119 posts that needed major security upgrades. It also determined that at some missions additional setback could be acquired through the purchase of neighboring properties.

Protecting the Perimeter

Setback is the preeminent security concern for our overseas posts. Setback provides the most protection from vehicle bombs. Since 1998 OIG has made recommendations that could effectively increase setback, some at a relatively low cost. For example, at one mission we recommended that officials work with the local government to alter traffic patterns around the mission. At another mission, we proposed creating increased setback by extending control over street parking spaces. However, at other missions the only way to effectively increase setback is to purchase adjoining properties, often at a cost of millions of dollars. In other cases, the mission itself must move to a new location to achieve any meaningful setback at a cost of hundreds of millions of dollars.

The $1.5 billion Emergency Security Appropriation has allowed the Department to begin to address the myriad security deficiencies. The type and level of security threats are constantly changing; posts are confronted with advances in technology that could render existing defenses obsolete; and the Department is faced with a budget that challenges its ability to ensure the safety of its people, information and facilities.

The ideal embassy would be protected not only by at least 100 feet of setback. It would also be constructed to current security standards and have a well-lit, well-constructed perimeter wall, and it would be under constant surveillance by closed circuit television. Beyond the wall, a surveillance detection unit would determine whether possible terrorists were surveilling the mission. A local guard force would guard the perimeter. Entrance to the mission compound would be well controlled. The chancery would incorporate a number of physical security measures to protect against bomb blast and to offer safehaven if the compound was breached. (See Appendix, Figure 1.)

Overseas Security Policy Board standards provided the framework for the OIG security oversight inspections we conducted over the last 18 months. Let me emphasize that none of the 42 embassies the OIG inspected during FY 1999 met all security standards. (See Appendix, Figure 2.) Thirty-four of those inspected do not have the required 1 00-foot setback to mitigate the damage of a vehicle bomb attack. Only 5 of the 42 posts have a new chancery under construction or planned in the next 5 years. Incremental security improvements such as upgraded walls, doors, and windows cannot fully compensate for the lack of sufficient setback. In addition, over 50 percent of the posts did not meet standards for window protection, perimeter walls, vehicle inspection areas, chancery wall and door construction, or exterior lighting and closed circuit television.

While many embassies or consulates we reviewed did not meet the minimum standard of a 1 00-foot setback to minimize a terrorist bomb attack, other physical security upgrade programs and projects have been initiated by the Department to improve building and perimeter security. In a significant number of our reports, we made recommendations to correct or improve perimeter security weaknesses or in some cases speed up completion of security enhancement projects planned or in progress.

At about one-third of all locations reviewed, we recommended measures to upgrade security barriers, exterior lighting, and anti-climb fences; install vehicle barriers at entry gates; revise local guard vehicle access control procedures; and upgrade public access control. In addition, we reviewed local guard services and recommended program improvements or greater post management supervision at about one-third of all locations. At six locations (14 percent) we felt it necessary for the post to increase the number of guards and/or services provided.

To mitigate the effects of flying glass resulting from a car bomb attack, the Department is replacing old and often defective 4-mil shatter resistant window film with a higher standard of protection. While the Department concurs with the ARB that ballistic laminated windows provide superior protection against a car bomb attack, the majority of our overseas facilities cannot structurally support this upgrade. A more practical solution is to purchase and install on all windows 8-mil shatter resistant film, which provides a measurable improvement in protection against flying glass and debris. All chanceries should meet the new 8-mil shatter resistant window film requirement by July 1, 2000.

Embassies Dar es Salaam and Nairobi

The OIG conducted a security evaluation at interim Embassies Dar es Salaam and Nairobi in May 1999 to determine the status of the Department's efforts to reestablish secure working environments following the August 7, 1998, terrorist bombings. While Embassies Dar es Salaam and Nairobi are more secure than at the time of the August 1998 bombings, both interim facilities still faced problems at the time of our May 1999 security evaluation. Embassy Dar es Salaam lacked sufficient emergency power for security systems such as exterior security lights, alarms, and vehicle barriers. Embassy Nairobi needed to reduce the risk of exposure presented by the placement of large glass windows in the front of the interim chancery building and provide a secondary exit point from the compound. The Department has corrected the emergency power problem at Embassy Dar es Salaam, and the large glass windows have been replaced at Embassy Nairobi.

Our evaluation of the interim office buildings for Embassy Dar es Salaam and Embassy Nairobi reviewed the management challenges that must be addressed to provide secure facilities and better protect employees of the Agency for International Development (USAID). Foremost among our concerns for the interim office buildings is the lack of co-location and the imminent need for the Department to address the security concerns that OIG has raised for those agencies that are not located on the interim office building compound, such as the Foreign Commercial Service, the Centers for Disease Control, and the Library of Congress.

Protecting International Broadcast Facilities

We have also reviewed the adequacy of security safeguards and procedures to counter threats to personnel, national security information, and facilities at the International Broadcasting Bureau (IRE) sites in Germany and Prague in October and January 1999 respectively. For Germany, the most serious concerns that we raised focused on the guy wire pad anchors, as the supporting tower and antenna are located in an open field and can be easily accessed. In Prague, the Radio Free Europe/Radio Liberty office building lacks setback and is situated between two busy streets. In addition, numerous physical and

procedural security deficiencies were identified that the IBB is taking action to correct.

Emergency Preparedness and Crisis Management

The Department has implemented a number of initiatives that will enhance an embassy's ability to handle a crisis situation including new emergency alarms and drills, expanded emergency planning programs, and emergency communications. In many cases, management- supported procedural initiatives can improve embassy security without any expenditure of funds. The OIG has provided numerous cost efficient recommendations in the course of its inspections and audits. As an example, during our inspection of the temporary embassy compound in Doha, Qatar, in August 1999, the OIG cited the need for the post to establish a proactive working relationship with the host government's protective service to ensure a cooperative and timely response to a terrorist incident. We also recommended that the Embassy initiate war gaming scenarios and compound walkthroughs with the designated Qatari response force to better prepare them for a terrorist incident.

Imminent Danger Notification System

Shortly after the East Africa bombings, the OIG recommended the immediate creation of an imminent danger notification system (IDNS) for each embassy that could be activated by a local guard on an embassy's perimeter if the guard detected a possible vehicle bomb. We also recommended that all missions practice a "duck and cover" drill in which employees seek immediate protection under desks or other furniture upon audible warning of a potential vehicular bomb attack to prevent the risk of death or injury from flying glass and other debris. Admiral Crowe's report strongly recommended such drills. Since then, our inspections have encouraged posts to implement quickly the IDNS system and to drill regularly on "duck and cover" along with other emergency drills.

Surveillance Detection

The Department has also developed a worldwide surveillance detection program. The ARB report recommended increased surveillance vigilance as a significant deterrent to terrorists who are targeting our posts. The surveillance detection program's goal is to enhance the prospect of preventing terrorist attacks by recognizing and reporting preoperational surveillance directed against U.S. personnel and facilities abroad. In FY 1999, the Department allocated approximately $77 million for the program.

Although work on our report is not yet complete, preliminary results of our specific review of the surveillance detection program at 22 posts indicate the program emphasis on quasi- covert operations and information gathering needs further refinement. In addition, regional security officers need post-specific surveillance detection procedures for attack notification, emergency procedures, and thresholds for confronting suspected surveillance. In a newly issued Field Guide for Surveillance Detection Management and Operations, the Department has begun addressing these issues.

Emergency Communications

In October 1998, the Department initiated the Overseas Wireless Program (OWP) as part of its response to the bombings in Dar es Salaam and Nairobi. The goal of the OWP was to modernize emergency and evacuation radio programs at over 260 overseas posts by

December 31, 1999. To implement the OWP, the Department provided its Bureau of Information Resource Management $1 18.5 million out of the approximately $1.5 billion in emergency security appropriations.

In response to this initiative the OIG began a review of the OWP in September 1999 to determine how it will improve the emergency and evacuation security environment for U.S. missions and personnel overseas. Our report is not yet complete, and Department officials have not had an opportunity to comment on our initial findings, so our observations are tentative. We believe the OWP will serve to improve the security environment at posts overseas by providing newer, more sophisticated radio equipment and by creating, at some posts, a dedicated emergency and evacuation radio network where none existed before. However, at posts we visited, the installation of the OWP radio equipment did not necessarily translate into an operating emergency radio network. Post officials were often unfamiliar with how to use the radio equipment, and new emergency and evacuation procedures incorporating the new equipment had not yet been put in place. The OWP has also been unable to achieve its goal of completing all installations by the end of 1999, because of the difficulties in implementing such a large installation in so short a time period and problems in obtaining host nation approval for dedicated OWP frequencies.

Admiral Crowe's ARB report also recommended substantially expanded training in crisis management along with other measures that would improve the Department's capabilities to respond to post emergencies and to assist in the restoration of operations of an embassy that has been taken out of action by either a terrorist attack or a natural disaster. The OIG is currently auditing the Department's emergency action management and related capabilities. We expect to publish our findings and recommendations later this spring.

INFORMATION SECURITY

Some of the most difficult security issues to correct both domestically and overseas deal with information security. OIG has completed over 20 audits identifying vulnerabilities in information resources and security management..1 In many ways, improving information security may be a bigger challenge than improving physical security because many of the fixes involve personal behavior rather than technical equipment. To correct identified vulnerabilities takes sustained senior management leadership, technically qualified people, money, and a desire to do things differently.

1 See appendix for listing of OIG security oversight audits.

Protecting Classified Information at Main State

Our work is not restricted to overseas alone. Following several disturbing incidents, most notably the February 1998 incident where an individual wearing a tweed jacket removed sensitive documents from the Secretary's suite, my office was directed by the Senate Select Committee on Intelligence to "conduct a review of the State Department headquarters' policies and procedures for handling classified information and to submit a report to appropriate committees of Congress with any needed improvements..." Our report, issued in September 1999, was entitled *Protecting Classified Documents at State Department Headquarters* (SIO/A- 99-46).

Recent lapses at Main State clearly demonstrate that attention must be given to

address vulnerabilities in protecting vital information on the domestic front that the OIG identified last year. The Secretary's April 24 decision to transfer authority for the physical protection of sensitive intelligence related material from the Bureau of Intelligence and Research (INR) to the Bureau of Diplomatic Security (DS) implements a critical action that we recommended as essential to ensure proper safeguards for our most sensitive intelligence related information.

In my statement on May 11, 2000, before this Committee, I discussed the specific deficiencies that have perpetuated a lax security environment in the Department of State and that the OIG identified during the course of our review.

In summary:

Ineffective access controls in the Department left offices vulnerable to the loss or theft of sensitive information and equipment by unescorted, uncleared visitors and contractors.

Lack of adequate physical and procedural security measures in offices resulted in classified documents not being properly controlled and accounted for.

INR was not fulfilling its security function, and unit security officers in other bureaus were not enforcing security requirements.

Disciplinary actions for security violations did not serve as a deterrent in correcting poor security practices.

Although the Department has begun to address these specific physical and procedural security problems, what is needed is continuous vigilance by all Department personnel and an ongoing commitment to maintain and enforce the highest level of security awareness and compliance.

In addition to audits of Main State security, OIG has begun a new initiative to inspect domestic facilities for physical and procedural security. In September 1999, we inspected the Office of Cuba Broadcasting (OCB) in Miami as part of this effort, and we just completed an inspection of the Beltsville, Maryland, Information Messaging Center. Among the findings in the OCB report was the need to harden perimeter security protection at the vehicle entry point and a requirement to establish an information security program. Recommendations in the Beltsville draft report call for an upgraded information systems security program and trained information system security officers. The Department agreed with OIG's findings and is taking actions to address the security concerns.

Overseas Telephone Security

In our November 1999 audit report on overseas telephone system security, we found that the Department was spending $61 million to upgrade its overseas telephone systems, but it was not focusing on improving the security aspect of the systems. The common practice of foreign national employees controlling the computerized telephone switches at overseas posts exemplifies a weakness in the security of the systems. Practical solutions have been identified to protect secure telephone operations and sensitive information. Furthermore, the Department needs to establish plans to modernize telephone security overseas and request

the resources needed to act on the report recommendations to improve telephone security and protect sensitive information. The Department agrees with the majority of the OIG's recommendations and is conducting a cost-benefit analysis of the addition security gained for installing a dedicated telephone switch for use in the controlled access area of overseas chanceries.

The OIG recently consolidated our information technology and security resources into an Information Resources and Security Management Division (IRSM) in the Office of Audits to address key information technology issues facing the Department of State. This division will address emerging issues of interest in five areas: information management, telecommunications, information security, information technology human resources, and information warfare. The IRSM Division's strategic objectives are to ensure that:

> U.S. personnel, facilities, information, and material are more secure through the identification and correction of information security weaknesses and deficiencies.
>
> Systemic weaknesses in information systems and security management are reduced.
>
> Potential cost efficiencies and opportunities for streamlining information management activities are identified and best practices shared.

OIG's Office of Security and Intelligence Oversight is performing an audit of the Department's counterintelligence (CI) program. The audit focuses on (1) the Department's program for screening employees before assignment to posts considered "critical" for CI threat, (2) the Department's CI awareness program, and (3) the Department's policies and procedures for reporting contacts and relationships with foreign nationals. The report will be issued in the summer of 2000. Additionally, an audit of the Department's background security investigations program will begin later this year.

FUNDING AND MANAGING FUTURE CAPITAL INVESTMENT

Admiral Crowe recognized the price we have paid for the failure to invest adequately in a secure diplomatic infrastructure. The Department has mobilized resources across the board to begin projects funded in the $1.5 billion Emergency Security Appropriation and to implement Admiral Crowe's recommendations, though Admiral Crowe also called for sustained, multi-year funding totaling $10 to $14 billion over the next 10 years. OIG has evaluated the Department's management of the Emergency Security Appropriation through August 31, 1999.

Overall, we found that the Department has provided senior level attention to the management of resources to improve overseas security. The direct involvement of the Under Secretary for Management and the Security Oversight Board has provided focus for the overseas security enhancements and fostered coordination among the Department's bureaus.

The ARB was disturbed by the collective failure of the executive and legislative branches over the past decade to provide adequate resources to reduce the vulnerability of our missions abroad. The Crowe Report underscored that our recent supplemental appropriation of over $1.5 billion for security is only a first installment in a long-term strategy for protecting American officials abroad. I cannot agree more strongly with the

Board's caution that substantial, long-term investment in security must take place. If we are going to put our employees in harm's way, we must protect them.

There are many reasons for the vulnerable condition of many American posts abroad. Lack of funding obviously plays a role. For many years, the Administration had not requested sufficient funds to improve physical security. The Administration has requested $410 million in technical and perimeter security upgrades funding for FY 2001. In addition, the Administration has requested $134 million for physical security improvements and $500 million, including $50 million for USAID relocations, for new facilities at the highest risk posts. The FY 2001 request also includes advanced appropriations increasing to $950 million in FY 2005 to provide sustained funding for the improvements called for the ARBs. The ARB report estimated that $14 billion would be needed over 10 years for security upgrades.

The Department is reviewing OPAP recommendations on reinventing the method of funding and administering the design and construction of buildings overseas. An interagency group headed by the Deputy Assistant Secretary for Foreign Buildings Operations (FBO) is reviewing all aspects of this issue. In addition, the Department has contracted with a leading consulting firm to examine various funding options and ways to make FBO a more performance-based organization.

The size of our presence overseas must also be considered as we examine how best to protect officials overseas. NSDD-38 currently provides an ambassador and the Department the authority to control staffing. What is sometimes lacking, however, is the exercise of that authority and the Department's support to the ambassadors who use their authority to deny unjustified staffing requests. The right answer to "right-sizing" lies in providing the staffing, financial support, and security required to do the job that needs to be done.

Another technique sometimes suggested to deal with both right-sizing and security issues is "regionalization." In brief, this means consolidating in a single diplomatic establishment or office in a single country many of the diplomatic and administrative functions that otherwise might be distributed among several U.S. embassies in several countries. There are instances when regionalization makes sense because of the economies, efficiencies, and safety of operations that result. Sometimes it may make sense from a security perspective, especially if the operation can be located in the United States. The Bureau of Western Hemisphere Affairs has consolidated a number of administrative, financial, and logistics activities at a regional center in Ft. Lauderdale, Florida. Similarly, regional centers in Frankfurt, Germany, provide engineering support and information management services to the new embassies created in the 14 former Soviet republics. However, it does not always make sense from a security perspective. Such concentrations sometimes create larger, more inviting targets for terrorism. Embassy Nairobi, for example, hosted several regional offices.

"Co-location," in other words bringing together all the elements of an embassy under a single roof or on a single compound, is another technique that can effectively enhance security. It creates a single, more defensible perimeter and should be incorporated in the "design and build" stage of every new embassy project. Recent OIG work in Africa including security inspections of our embassies in Nairobi, Dar es Salaam, Luanda, and Kampala, strongly recommended the co-location of USAID and other elements into the planned mission compounds.

Strengthening Security Management

The ARB, in examining the embassy bombings in Nairobi and Dar es Salaam, concluded those security activities were hindered by a lack of a firm and recognized chain of accountability for security matters. As the OPAP report indicated, "Every President since John F. Kennedy, who created the "country team" concept, has issued a letter to each Ambassador reemphasizing the legal responsibilities and authority of Ambassadors and adding directives based on that President's personal goals for the mission. In recent years, with the rapid expansion in the number of U.S. Government agencies sending personnel overseas, the role of the Ambassador has not been clearly understood."

Other agency personnel often view the Ambassador as the Department's representative, rather than the President's. The Ambassador is left with the responsibility to coordinate the activities and address the often-competing needs of the mission. In an emergency, this can delay and/or prevent a timely and effective response. Mission chain of accountability must be clearly defined enabling the Ambassador to respond decisively and with full statutory authority in a crisis situation. To quote from the OPAP report, "today's ambassadors are "coordinators and consensus builders." I further agree with the OPAP Panel that "the Ambassador's authority over his or her mission should be reasserted and reinforced in a manner that takes account of the complex, interagency nature of that mission."

LOOKING AHEAD

Mr. Chairman, in your invitation to testify this morning, you asked that I address the ability of the Department to manage a security enhancement program and the status of various security initiatives. I have, therefore, focused my remarks on how the Department, including the Office of Foreign Buildings Operations, has responded over the last 18 months to the graphic demonstration in Nairobi and Dar es Salaam of just how vulnerable our diplomatic infrastructure has become. Those tragedies have captured the attention of the foreign affairs community, the Congress, and the American public. Meanwhile, recent security lapses at home have been a wake-up call that other aspects of security, just as vital to the defense of American interests as physical security, also need attention.

The Department has responded well to the need to move quickly in the aftermath of the bombings in East Africa and to use the emergency funding provided by the Congress to begin to enhance the security of our personnel, information, and facilities overseas. But we should not expect that we can ever provide absolute security of our representatives abroad. We should not expect that the threat to U.S. interests, from whatever quarter or in whatever form, can be eliminated.

The challenge for the Department of State is to establish a structure and implement a strategy that will address security comprehensively and for the long term. Long after these hearings, and long after the media attention has faded, the legislative and executive branches must remain committed to policies, programs, and funding that will sustain the continuous improvement of our foreign affairs infrastructure and our ability to respond and adapt to the inevitably changing nature of the threats against us.

The Department of State has an important but not an exclusive role in meeting this challenge. The Department's success is dependent on how well and for how long the foreign affairs community and the Congress remain committed to funding the construction, maintenance, and continual improvement of that infrastructure and a disciplined attention to effective security procedures and practices.

As the Department and the Congress embark on this expensive commitment, the requirement for the Office of Inspector General to provide specialized and expert oversight of the use of those funds for physical, procedural, and programmatic security enhancements also increases. As the Department moves from an emergency response to a more strategic process for building our foreign affairs infrastructure, so must the OIG adapt to and respond to the needs of the Congress and the Department for greater breadth, depth, and sophistication in our monitoring of these new initiatives.

With the exception of a small, one-time emergency supplemental appropriation in FY 1999, funding for the Office of Inspector General has been straightlined since FY 1996. Over the last 5 years we have absorbed the cost of mandatory requirements such as Law Enforcement Assistance Pay and Chief Financial Officer Act audits and all inflationary increases. Increased funding for security and for those charged with overseeing security improvements for you and for the Department is only one of the ingredients necessary for rebuilding infrastructure and changing attitudes toward security, but it is a vital ingredient for all of us.

Mr. Chairman, I hope that as the Congress and the Department work together in response to these challenges, that we in the OIG also receive the support necessary to play our important role as well.

BIBLIOGRAPHY

Audit of Overseas Telephone Systems Security Management, SIO/A-00-01, November 1999

Protection Classified Documents at State Department Headquarters, SIO/A-99-46, September 1999

Information Assurance, November 1998 Memo to P

Declassifying State Department Secrets, SIO/A-98-50, September 1998

Audit of the Management of Sensitive Compartmented Information (SCI) Access, SIO/A-98-49, September 1998

Audit of the Management of Secure Communications, SIO/A-97-15, March 1997

Audit of the Classified (Red) Mainframe System's Security, SIO/A-97- 02, October 1996

Report on FSC Bangkok Access Control and Operating System Security, OSO/A-96-16, May 1996

Protection of Classified Material at Embassy Wellington, OSO/A-96- 11, January 1996

Audit of Unclassified Mainframe Systems Security, OSO/A-96-10, January 1996

Followup Audit of Domestic Telephone Security, OSO/A-95-25, July 1995

Letter of Findings on the Onyx System's Access Control and Operating Systems Security, December 1994

Letter of Findings on the Black System's Access Control and Operating System Security, November 1994

Letter of Findings on RAMC - Bangkok Access Control and Operating Systems Security, OSO/A-94-40, August 1994

Letter of Findings Audit of RAMC - Paris Access Control and Operating Systems Security, OSO/A-94-21, June 1994

Audit of Overseas Technical Security, OSO/A-94-02, October 1993

Office of Security Oversight Audit of Domestic Telephone Security, OSO/A-93-12, March 1993

Office of Security Oversight of the Control and Accountability of Cryptographic Equipment and Material, OSO/A-92-24, June 1992

Audit of the Bureau of Intelligence and Research Automated Information System Security, OSO/A-91-22, August 1991

Security Oversight Audit of Overseas Computer Security, OSO/A-90-27, September 1990

Figure 1. Elements of Embassy Protection

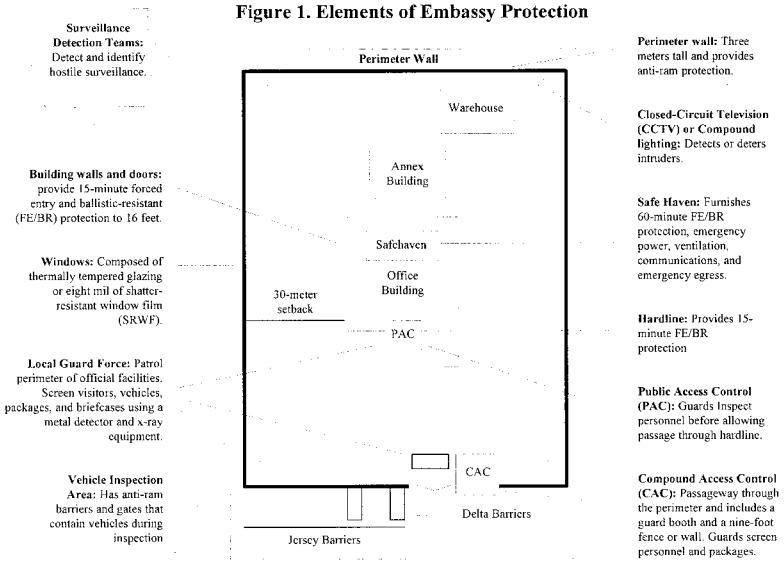

Figure 2. Overseas Posts Compliance with Security Standards

	Adequate	Percent	Inadequate	Percent	N/A
Setback	8	19	34	81	
Windows	11	26	31	74	
Perimeter Walls	12	29	28	67	2
Compound Access Control	17	40	18	43	7
Vehicle Inspection Area	18	43	23	55	1
Chancery Walls and Doors	20	48	22	52	
CCTV/Lighting	20	48	22	52	
Safehaven	25	60	17	40	
Public Access Control	31	74	11	26	
Local Guard Force	36	86	6	14	
Surveillance Detection	14	33	2	5	26

Note: The surveillance detection program began after the bombings in East Africa;consequently, it did not exist at posts inspected early in FY 1999.