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, I 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 officers 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 constru to current security standards and have a well-lit, well-constructed perimeter wall, and it would be under consta surveillance by closed circuit television. Beyond the wall, a surveillance detection unit would determine whet possible terrorists were surveilling the mission. A local guard force would guard the perimeter. Entrance to th 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 100-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 100-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 $118.5 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.

Protecting Classified Information at Main State

Our work is not restricted to overseas alone. Following several disturbing incidents, most

[1] See appendix for listing of OIG security oversight audits.

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 additional security gained from 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.

Without belaboring the point with you 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 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.

Figure 1. Elements of Embassy Protection