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[1] 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.