United States Department of State
Office of Inspector General

Security and Intelligence Oversight Audit

PROTECTING CLASSIFIED DOCUMENTS AT STATE DEPARTMENT HEADQUARTERS

SIO/A-99-46

SEPTEMBER 1999

OFFICE OF INSPECTOR GENERAL

OFFICE OF SECURITY AND INTELLIGENCE OVERSIGHT

PROTECTING CLASSIFIED DOCUMENTS AT STATE DEPARTMENT HEADQUARTERS

EXECUTIVE SUMMARY

This Office of Inspector General (OIG) audit report addresses the effectiveness of State Department policies and procedures for protecting classified documents at the Main State Headquarters facility, in Washington, D.C. The Senate Select Committee on Intelligence (SSCI) directed OIG to conduct the review in response to several reported incidents of lax security.

This audit concluded that programs are in place to evaluate individuals' trustworthiness and need to handle classified information. Likewise, physical and procedural safeguards are in place to protect information from unauthorized disclosure to individuals who do not have a demonstrated need for access to national security information, particularly material related to intelligence. Nevertheless, the level of security awareness and controls to prevent unauthorized disclosures could be substantially enhanced. Specifically:

Very highly classified documents relating to intelligence reporting are not safeguarded in accordance with Government regulations. Most offices have never been inspected and accredited for handling such documents. A significant number of foreign nationals are permitted unescorted access to the Department. [(b)(2)----------]

- Administrative actions taken to discipline employees are ineffective to ensure that poor security practices are corrected. Unit security officers are not well informed about security requirements and do not have the authority to enforce security requirements.

The OIG recommends that the Bureau of Diplomatic Security (DS) be designated as the organization responsible for protecting SCI and that DS enhance physical and procedural measures required to safeguard such information. The Department should implement a policy that provides greater control over visitors to the Main State building. Access controls to facilities where classified information is handled, processed, and discussed should be enhanced. Disciplinary actions and training should be strengthened to reduce the frequency of security incidents. If implemented the recommendations contained in this report would improve security at Main State.

Department Comments

OIG staff provided copies of the draft report to DS and the Bureau of Intelligence and Research (INR) and met separately with officials from each bureau. DS officials reviewed the draft of this report and agreed with the findings and recommendations. The bureau's primary concern was that in order to implement the recommendations, DS must be formally designated as the security office for intelligence information security, and DS would require additional funding.

INR officials said that the bureau agreed with the finding that security policies are not being suff~ciently enforced. INR management did not agree with the recommendation to designate DS as the cognizant security Officefor the protection of SCI. INR also has a different interpretation of some security directives and believes that certain offices need not be fully accredited for discussing and handling SCI. INR also suggested that OIG had exaggerated the extent to which SCI is mishandled. INR's written comments are contained in Appendix A. The OIG's responses are found in relevant sections of the report.

OFFICE OF INSPECTOR GENERAL

OFFICE OF SECURITY AND INTELLIGENCE OVERSIGHT

PROTECTING CLASSIFIED DOCUMENTS AT STATE DEPARTMENT HEADQUARTERS

TABLE OF CONTENTS

1. OBJECTIVES, SCOPE, AND METHODOLOGY

This audit was initiated by the Office of Inspector General (OIG) in response to the FY 1999 Intelligence Authorization Act, which required the OIG to ". . . conduct a review of State Department Headquarters' policies and procedures for handling classified information, and submit a report to the appropriate committees of Congress with any needed recommendations for improvements ...." Congress requested the audit as a result of several reported instances where highly classified information was unaccounted for. In one instance, reported in February 1998, an individual wearing a tweed coat removed classified documents from the Secretary's suite. The individual in this "tweed coat" incident has not been identified.

In accordance with that legislative requirement, the OIG identified the following reportable issues:

1. Is classified information handled, disseminated, and stored in a manner consistent with Government regulations, and that minimizes the likelihood of unauthorized disclosure?

2. Are Main State access controls and escort procedures adequate for protecting classified information?

The audit field work was performed in Washington, D.C., between August 10, 1998, and April 30, 1999, with the Office of the Secretary (S) and the bureaus of Intelligence and Research (INR), Diplomatic Security (DS), European Affairs (EUR), South Asian Affairs (SA), Near East Asian Affairs (NEA), and Personnel (M/DGP).

In evaluating policies and procedures for protecting classified information, the audit focused on classified documents that contained sensitive compartmented information (SCI) by reviewing INR document control procedures and a sample of procedures in six headquarters offices to assess handling procedures for all classified documents. The audit focused on the handling of hardcopy documents and did not address the possible vulnerabilities associated with electronic data transmission and storage.

The OIG interviewed DS officials responsible for the security incident program, access controls, guard force, and investigations; INR security personnel responsible for SCI security; and other INR intelligence analysts, document control officers, and senior managers. The OIG monitored document distribution and access control procedures.

The audit team reviewed all pertinent Department regulations and Director of Central Intelligence directives (DCIDs) for the protection of documents, reviewed Department compliance with those directives, examined security awareness briefings and other instructional methods to evaluate their effectiveness in motivating employees to protect classified information. The audit team also submitted questionnaires to cleared Department employees to solicit their views on Department procedures for protecting classified information and attitudes toward such procedures.

The team interviewed Federal Bureau of Investigation (FBI) staff responsible for investigating counterintelligence matters and unauthorized disclosures of classified information, and Central Intelligence Agency (CIA) officials responsible for promulgating Government-wide intelligence community standards for safeguarding SCI and for accrediting SCI facilities (SCIFs).

The auditors compared the level of security and assessed the division of responsibilities for protecting classified documents among DS, INR, and the functional bureaus by interviewing responsible officials, and by examining work requirements statements and actual duties performed. The audit was conducted in accordance with generally accepted auditing standards by James Martino (audit manager), Thomas Boots, Stephanie Hwang, and Mary Siatis.

II. BACKGROUND

The Department of State handles, processes, and stores thousands of classified documents each day at overseas posts and at the Main State headquarters building. Countless meetings are held where classified information is discussed. Gathering, analyzing, and distributing information is central to the Department's mission to implement U.S. foreign policy. This information routinely includes national security concerns such as intelligence information, sensitive matters relating to bilateral and multilateral relations, and other national security issues. The information is disseminated through a variety of media, including electronic mail, computer systems, hard copy, telephone, fax machines, and meetings.

Regardless of the means by which such information is disseminated, it is essential that it be limited to authorized personnel with appropriate security clearances who have been adequately briefed on protecting such information. Compromising classified information— inadvertently or intentionally—particularly highly classified intelligence information, could result in:

- the loss of vital sources of information to U.S. policy makers and military planners;
- the arrest, torture, or death of sources or other individuals;
- the waste of huge outlays of funds for research and development of data collection methods; and
- serious damage to the Government's relationships with other governments.

The Department acknowledges the threat to national security and has established policies and procedures to minimize the potential compromise of classified information. Employees and contractors receive background investigations before being cleared to handle classified information; there are guards and access controls - at the perimeter entrances to Main State and in many offices; procedures are in place for distributing classified material to individuals; employees receive briefings on handling classified information; and there are procedures in place for identifying individuals who violate security protocols.

Department regulations require that the executive director of each bureau ensure that a principal unit security officer (PUSO) is designated. The USO's duty is to make sure classified information is handled according to regulations, and to work with office staff to ensure that all employees are aware of security requirements and procedures. By regulation, the ultimate responsibility for safeguarding classified information rests with each organizational unit supervisor. The Foreign Affairs Manual (FAM) also states that "each employee having access to and/or possession of classified material is responsible for the maintenance of the security of such material."

The OIG recognizes that there is an inevitable tension between those charged with collecting and protecting intelligence information and those who must use that information to formulate and conduct foreign policy.

This report describes Department policies and procedures for protecting classified information at the Main. State headquarters building, and the extent to which security measures have been effective in preventing the unauthorized disclosure of classified information.

III. FINDINGS AND RECOMMENDATIONS

A. DEPARTMENT COMPLIANCE WITH DCI DIRECTIVES FOR PROTECTING SCI DOCUMENTS

The Department is substantially *not* in compliance with the DCIDs that govern the handling of SCI. The Assistant Secretary of INR' is the Department's senior official of the intelligence community (SOIC) (1 FAM 431) and as such is required to oversee the Department's efforts to protect SCI and to ensure that SCI is handled in accordance with DCIDs. The primary reason for noncompliance with DCIDs is that INR's primary mission is not security and it does not have the resources to meet its multiple responsibilities of acquiring, analyzing, disseminating, and protecting SCI information. DS, on the other hand, as mandated by the Omnibus Diplomatic Security and Antiterrorism Act of 1986 (Public Law 99-399), has the responsibility to provide security to the Department abroad and domestically, which includes the protection of classified information up to and including the top secret level. Dividing the responsibility for protecting SCI and classified information between INR and DS has not been effective. As a result SCI is regularly handled without adequate protection or accountable controls.

INR's Responsibilities

INR is the recipient and controller of SCI and manager of certain special access programs. The Assistant Secretary of INR as the Department's SOIC, is responsible for implementing DCIDs including those covering the protection of SCI (Executive Order [E.O.] 12333, December 4, 1981). The SOIC, for the purpose of SCI protection and DCID implementation, is considered the equivalent of the head of a-cognizant security agency. DCIDs 1/14, 1/19, and 1/21 establish many of the physical and procedural security requirements for protecting SCI to which all intelligence community agencies must conform. The responsibility for implementing DCID security requirements resides with the SOIC's INR security unit. For Department employees, INR requests DS to review employees' security files to determine eligibility under the standards for SCI access; INR grants or denies SCI access and provides the security awareness briefings. INR can grant waivers for SCI access. The Director of Central Intelligence (DCI) gives the SOIC the authority via DCID 1/19 to *"delegate responsibility for the implementation of policies and procedures defined in an appropriate DCID... to a Cognizant Security Office"* (DCID 1/19). In other words, the SOIC can establish a security unit within INR or delegate that responsibility to another entity, such as DS.

As reflected in the INR FY 1999-2000 Program Plans Statement, the bureau's primary mission is to acquire, analyze, and disseminate intelligence. INR is to provide four core services to the Secretary of State; senior Department policy makers and chiefs of mission; and, to some extent, the DCI:

- Provide current intelligence and warning by maintaining a 24-hour watch.

'The National Security Act (Public Law 80-253) includes INR as part of the intelligence community.

- Provide independent, all-source analysis through written and oral briefings and the *Secretary's Morning Intelligence Summary* every day of the year.
- Assist the Department and chiefs of mission to coordinate intelligence activities such as border security, coordinate collection activities with the intelligence community, and develop Department positions on counterintelligence, covert action, law enforcement, and other sensitive issues.
- Support the Secretary and DCI by representing the Department's interests in policy forums on issues such as budgeting and resource issues, and advising the DCI on intelligence reform, diplomatic support, and intelligence policies.

DS's Responsibilities

The FY 1999-2000 Program Plans Statement for DS notes that the bureau's primary mission is to provide a secure working environment for the conduct of foreign affairs through a commitment to the protection of life, information, and property. The mission includes:

- Physical and technical protection of the domestic and overseas facilities of the Department.
- Protection of the Secretary of State and other senior government offrcials, visiting foreign dignitaries, and foreign missions in the United States.
- The integrity of international travel documents, sensitive information, and management information systems.
- Criminal, counterintelligence, and personnel security investigations.

According to Department regulations (12 FAM 512.1-3(b) 1 through 11), DS has primary responsibility to oversee the Department's information security program and ensuring the protection of classified information—including intelligence information—from unauthorized disclosure. The Assistant Secretary of DS is responsible for establishing and implementing policies for the protection of classified information up to and including the top secret level at overseas posts and domestically.

Department Compliance with DCID Requirements

The Department does not protect SCI information in accordance with DCID requirements. Specifically, SCI documents are regularly introduced into offices that have not been accredited for handling or discussing SCI, are not always properly stored, and are not properly accounted for.

Unaccredited Offices

Most offices in the Department where SCI is routinely read and discussed have not been inspected or accredited to handle SCI, as required by DCID 1/21. INR offices where SCI is received, analyzed, and stored have been inspected and accredited. [(b)(2)----------]. In cases where work areas have not met DCID standards, a waiver must be approved by the agency SOIC in writing and notification provided to the DCI. The expectation of the Security Policy Board is that when

physical measures are not sufficient, compensating procedural measures should be adopted and awareness of proper security practices should be reemphasized.

The Department has 39 accredited SCIFs for storing, handling, and electronic processing of SCI information. SCI is routinely delivered, however, to approximately 140 other offices that have not been inspected and accredited to handle SCI.

SCI material is received by INR from other intelligence agencies by pouch or electronically. INR uses this material to produce SCI material such as the *Secretary's Morning Intelligence Summary.* Such products are distributed to 140 Department addressees by pouch: INR analysts brief Department employees in 94 non-accredited offices while retaining custody of the SCI material, and pouches are delivered to 46 non-accredited offices to be returned by close of business to INR. Upon return, the pouches are "stripped" by INR personnel, and the SCI material is destroyed or stored in safes in INR SCIFs.

Before introducing SCI into non-accredited offices, security personnel are required to conduct inspections of the Office space to determine if physical or procedural controls meet DCID standards. If those standards are not met, a waiver must be sought. The DCID also requires that the cognizant security authority conduct periodic inspections of accredited offices to oversee security controls.

INR has issued letters authorizing 33 of the 140 offices (without being inspected and formally accredited) as Temporary Secure Working Areas (TSWAs) to receive, but not store, SCI. These letters were issued to remind employees that ". . . at the end of the business day, the pouch must be returned with all of its contents to INR." DCID 1/21 states that TSWAs can be designated for up to 40 hours per month and for a maximum of 6 months. INR has permitted SCI into these TSWAs on a daily basis for years without appropriate waivers. The TSWA designation is for exceptional cases and for brief periods, not for routine business.

The 140 offices where SCI is handled and discussed have not received technical surveillance countermeasure inspections. The purpose of these inspections is to determine whether listening devices have been surreptitiously introduced. DCID 1/21 (3.2.2) states that these inspections may be required at the discretion of the cognizant security authority. All personnel in these offices should be cleared to the SCI level, and, if not, uncleared employees should be monitored. [(b)(2)----------]

SCI Not Properly Stored

Some SCI documents distributed by INR to Department offices during working hours are not returned to SCIFs for storage by close of business as required by DCID 1/21. According to the chairman of the Security Policy Board's Facilities Protection Working Group, under no circumstances should of fices be allowed to store SCI material outside of a SCIF overnight.

The OIG reviewed records for top secret SCI documents maintained by the Cryptological Support Group, a National Security Agency (NSA)[2] liaison Office in Main State, [(b)(2)---------- -- ------] between August 19, 1998, and October 19, 1998. This review showed that 239 (12.6 percent) of 1,890 documents delivered during this period had not been returned to the Cryptological Support Group SCIF. A review of INR Office of Security records showed cases of SCI material discovered after hours outside a SCIF and of pouches containing SCI that were delivered to non-accredited offices, and not returned to INR by close of business. INR watch office personnel also cited instances of pouches with SCI material that were not returned to the INR watch Office SCIF after hours.

SCI Not Accounted For

INR does not track SCI documents distributed to non-accredited offices as required by DCID 1/19 section 6.10. Responsible officers are required to obtain signed receipts for SCI released in this manner and to ensure that conditions of use will provide adequate security until the SCI is returned to a SCIF.

Daily, an estimated 3,500 pages of SCI are distributed to 46 non-accredited offices. Although a standard distribution list for pouches assembled by the INR watch indicates which addressee should receive what material, there is no record of what material was actually delivered or if the material has been returned. [(b)(2)--- -- -- --- -- -- ----]

INR's Principal Mission and Security Responsibilities

INR's principal mission is analysis and research for the Secretary, 7th floor principals, and senior policy staff. In an attempt to strike a balance between disseminating the information and ensuring that proper security practices are followed, INR management has made the timely and efficient distribution of information a high priority.

The INR Office of Security's primary security functions are granting and tracking SCI clearances, conducting SCI awareness briefings, and investigating SCI security incidents. The INR security Office has not provided the day-to-day management of SCI handling required by DCID 1/19, such as ensuring that SCI is properly controlled, tracked, transmitted, packaged, safeguarded, and destroyed.

INR and DS personnel are aware of improper handling of classified material. Senior Department officials' needs to review current intelligence information in a timely manner

2 NSA has a system of tracking certain documents delivered to the Department whereas the Department does not track the SCI documents it receives.

sometimes outweigh the need for strict adherernce to security requirements. Based on OIG's interviews with Department officials and the responses to an employee questionairre, there is a general belief among SCI users that secuirty measures at Main State are sufficient to deter a hostile attempt to acquire the information.

INR has not effectively discharges its responsibilities for the protection of SCI. The primary mission of INR is to analyze and distribute intelligence information to Department officials in support of U.S. Foreign Policy. A secondary concern is ensuring that the information is handled in accordance with security regulations. In OIG's view, INR is not well suited to oversee the day to day management of SCI security. To some extent the desire to efficiently distribute SCI conflicts with the need to properly safeguard the information. The primary function of DS is to ensure that people and information are properly protected as is clearly established in 12 FAM 512. DS has a cadre of trained security professionals who are knowledgeable about the physical and procedural procedures for protecting classified material and are responsible for overseeing Department procedures for protecting classified information up to the Top Secret level. Responsibility for safeguarding SCI should be delegated to DS.

Recommendations

The OIG recommends that the Assistant Secretary for Intelligence and Research:

1. Designate DS as the Cognizant Security Office for the protection of SCI. [Action: INR]

The OIG recommends that the Assistant Secretary for Diplomatic Security:

2. Inspect and accredit all offices where SCI is handled, and make all the physical and procedural security enhancements required to safeguard SCI. Any waivers to DCIDs should be formally transmitted to the DCI. [Action: DS]

3. Implement procedures to ensure that SCI documents are returned to SCIFs each night. [Action: DS]

4. Establish controls for SCI documents removed from SCIFs that are in compliance with DCID 1/19. [Action: DS]

INR Comments and OIG Analysis

INR stated that the DCIDs do not require the accreditation of offices where SCI material remains under the constant visual protection of INR officers while briefing Department officials in their work areas. They further asserted that offices can be accredited as TSWAs provided that pouches are returned to INR by close of business. OIG discussed this point with the Community Management Staff (responsible for DCID developments for all agencies). The chair of the Counterintelligence and Security Team reaffirmed to OIG that Community Management Staff policy is that all offices must be accredited where SCI is introduced, even if SCI is presumably only discussed, and that SIC must not be routinely allowed into TSWAs for all day use. According to DCID standard, SCI can be handled in such offices for not more than 40 hours per month. TSWAs are intended for brief periods of use and not for routine, sustained work. Temporary accreditations should be for a maximum of 6 months.

INR also challenged the OIG finding that 12.6 percent of NSA documents distributed to [(b)(2)----------]were not being returned to CSG. INR said that the documents in question were returned to the [(b)(2)----------] each night. OIG finds no basis for this supposition. The established procedure for [(b)(2)----------]was to place the NSA documents into their pouch at night; these pouches were to be delivered to the [(b)(2)----------]—collocated with CSG—which in turn place the documents in a burn bag for destruction. The documents in
question were not returned to CSG. INR's position that the documents were returned to the INR front office SCIF cannot be confirmed because INR did not know which documents were not returned to CSG, INR has no means of tracking such documents, and [(b)(2)----------]are not instructed to return the documents to the INR front office. OIG auditors were told by the chief of the CSG that she was unaware of the location of the NSA documents if not returned; furthermore, she stated that when Department officials rotate to other assignments they routinely return to CSG bundles of NSA documents that may or may not have been stored in accredited SCIFs (Note: none of the [(b)(2)----------]

B. ESCORTING VISITORS AND CONTRACT EMPLOYEES

Department policy allows many visitors to the Department to move about unescorted if they have been cleared to enter the building. As a result, visitors are unaccompanied while proceeding to areas where classified information is discussed, handled, and processed. The Department should exercise greater control over the movements of such visitors. A new visitor escort policy to create such controls has been proposed, but not implemented.

[(b)(2)----------] The Department
requires that uncleared personnel be escorted in areas where classified work is being conducted or classified materials are stored. [(b)(2)----------]

Criteria

The Department's visitor policy authorizes dependents, foreign officials, conference attendees, other government employees, VIPs, media representatives, and other private citizens to move about State Department headquarters without escort. In November 1995, the Under Secretary for Management approved a new policy proposed by DS to exercise greater control over such visitors. The "New Visitor Escort Requirements" policy was issued as a Department Notice stating that ". . . all visitors, with the exception of active US Government agency personnel who display proper photo identification, shall be escorted at all times." The announcement was withdrawn shortly thereafter for further review.

The Department requires that uncleared personnel be escorted when in classified areas. According to a DS official, it is the responsibility of employees to ensure that contractors entering their offices have the appropriate clearances and, if not, that they be escorted, at all times.

Visitors Are Not Controlled

A DS survey of visitors recorded in the visitor log book during a 4-week period showed that 14 percent of the visitors were foreign government offtcials, 22 percent were U.S. Government employees, and 63 percent were private American or foreign citizens. According to DS officials, approximately 1,000 people visit the Main State Department building each day, yet the number varies significantly. OIG's spot check of the visitor log on September 8 and 29, 1998, showed there were 1,726 visitors over the 2-day period of which 326, or 19 percent, were foreign government offcials. Once cleared to visit and issued a visitor's pass, most visitors move about the building unescorted.

Pre-clearances are granted to visitors using a written pre-admittance form for visitors attending conferences or tours and visiting Department employees. Employees provide the Department's reception desk with completed "Pre-Admittance Authorization Forms" listing information about the visitor including name, birth date, citizenship, and sponsor's name. Visitors show identification to the receptionist, who then checks the visitors' names against the forms submitted. Visitors are logged in the visitors log, given a visitors badge, and admitted into the building. Visitors not previously identified to the receptionist are cleared to enter after a telephone call to the visitor's destination or if the visitor arrives with a Department employee having escort authority. The visitors show the receptionist identification, sign the visitors log, receive a visitors badge, and proceed into the building.

Some VIPs and dignitaries are escorted for reasons of protocol. Others proceed to their intended destination unescorted. Visitors cleared after hours are escorted to their destination by guards or other individuals with escort authority. On departing the building, visitors are expected to return visitors badges to a guard stationed at one of the four building entrances.

Escort of Maintenance and Repair Personnel and Char Force

[(b)(2)----------

----------]

According to DS, there are approximately 350 contractors and the vast majority are uncleared. For example, an equipment maintenance contract provides 35 employees yet only 9 employees have clearances; a custodial services contract provides approximately 100 employees of which 15 have clearances.

[(b)(2)---------- ---------- ----------]

Escorting is Burdensome

The Department allows unescorted movement in Main State because the expectation is that once these individuals reach their stated destination, cleared American employees will escort them in sensitive areas and that employee escorts will be diligent in monitoring the visitors' whereabouts. Department officials contend that a requirement to escort all uncleared visitors throughout the building would be too burdensome.

Unescorted Access is a Security Vulnerability

Visitors are allowed unescorted access into the Department, and [(b)(2)---------- ----------] A recent FBI report stated that suspected foreign intelligence personnel were granted unescorted access. The policy of allowing unescorted access poses a significant security vulnerability for the surreptitious planting of listening devices, theft of documents or overhearing discussions of classified information.

Recommendations

The OIG recommends that the Undersecretary for Management:

5. Implement a visitor escort policy whereby any visitor without a U.S. Government security clearance is escorted at all times while in the Main State facility. [Action: M]

6. [(b)(2)---------- ----------]

C. IDENTIFICATION BADGE SYSTEM

The Department employee identification badge system has been improved since the "tweed coat" incident, but further improvements are necessary. The Department's current system does not meet DCID requirements on SCIF access control and makes unauthorized access to the building and to classified work areas feasible.

Criteria

In selecting the new badge reader system for Main State, the Department required compliance with Underwriters Laboratories (UL) codes. The system stores information on several servers to ensure redundancy so that card readers can continuously read and record who enters and leaves the building. The system can be programmed to read badge expiration dates and deny access to expired badges.

The Department is also seeking to attain "smart card" capability for its automated badge system. Smart cards (the administration advocates government-wide application) contain computer chips and can be used for a wide range of functions other than building access, including travel, word processing, purchasing, and medical information.

DCID 1/21 requires that the automated access control system for a SCIF must identify an individual and authenticate that person's clearance for access. Authentication can be by the use of personal identification numbers (PINs) 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."

Department Badge System

The Department issues identification badges to all employees with a need to enter Department facilities. As of April 1999, new card readers using the Monitor Dynamics, Inc. (MDI) system were installed throughout Main State, replacing the old "Cardkey" system. The MDI system significantly improves the reliability of the badge system that was in place at the time of the "tweed coat" incident. MDI provides the Department with the ability to proceed to implement smart cards and biometric card readers.

[(b)(2)----------
---------- -]
The Department relies on this badge for access control into SCIFs and classified work areas. For SCIF areas in the Department, DCID 1/21 requires badge systems to verify an individual's identification unless the SCIF entrance is under visual control at all times during duty hours.
[(b)(2)---------- ----------
---------- ----------]

DS officials stated that biometrics will be effective in areas where tighter access controls are needed, such as SCIFs, TSWAs, and classified and open storage areas, and that DS has successfully tested hand geometry. DS proposes to install such a system for some INR offices and has submitted a cost estimate to INR. INR has not yet responded to their proposal.

The Department's badge system has been improved, but is still deficient. The application of smart card and biometrics technology has not been fully examined. [(b)(2)----------
----
----------] Given the amount of classified material dispersed throughout Main State, the possibility of unauthorized access in sensitive areas is sufficiently high to warrant tighter controls.

Recommendation
The OIG recommends that the Assistant Secretary for Diplomatic Security:

7. Install biometric access controls at SCIFs and other sensitive offices where entrances are not under constant visual control. [Action: DS]

D. SECURITY INCIDENT PROGRAM

The security incident program is intended to identify improper security procedures and to educate employees in the proper safeguarding of classified information.[3] During the 4 years from 1995 through 1998, 53 cases were referred to the FBI for unauthorized disclosure of classified information; 1,673 security incidents were issued at Main State in 1998. Infractions were not issued when INR's procedures on handling SCI were not followed; INR's practice was to retrieve mishandled documents and brief employees on the proper security procedures. DS has provided security briefings for unit security officers and sponsored a town meeting to discuss employee security responsibilities. Yet employee security awareness and concern about the proper handling of classified material is low because awareness training has not been sufficient and the administrative actions taken to discourage the improper handling of classified information are not effective. Therefore, classified information is vulnerable to intentional and inadvertent disclosure.

Criteria

As the SOIC for the Department of State, the Assistant Secretary for INR is responsible for ensuring that the DCIDs, governing eligibility for access to SCI material, are followed and are consistent with the interests of national security. This responsibility includes assurance of the control and protection of intelligence information on a need-to-know basis. The INR security officer is responsible for ensuring that intelligence information is properly protected in the Department.

The Assistant Secretary of DS's primary responsibility for overseeing the Department's information security program includes the:

- protection against unauthorized disclosure of classified information, including intelligence information,
- and establishment of a security awareness program to educate employees concerning their duties and responsibilities with regard to the requirements of E.O. 12958.

Guards conduct after-hours security inspections and issue security incident reports. Security incidents are forwarded to DS for adjudication. Disciplinary action may include:

- a letter of warning;
- a letter of reprimand;
- suspension without pay; or
- dismissal.

---

3 A security incident is a failure to safeguard classified materials in accordance with regulations and can be either an infraction or a violation. An *infraction* occurs when information was not properly safeguarded but does not result in the actual or possible compromise of the material. A *violation* occurs when the failure to safeguard information *could* result in the actual or possible compromise of the material. In 1998, there were 4 incidents characterized as violations at Main State, and 1673 infractions.

Security incidents are counted over an 18-month period. During this moving timeframe repeat security violators are referred to M/DGP for possible disciplinary action.

Security Incident Program

Despite the security incident program, there have been a number of unauthorized disclosures the Department referred to the FBI for possible criminal prosecution, and there were repeat security offenders. Marine security and contract guards issued 1,673 security incidents primarily at the "confidential" and "secret" level in 1998. There were 6 incidents reported involving SCI material.[4]

When unauthorized disclosure of classified information is suspected, the case is referred to the FBI for prosecution.s The Department referred 3 cases to the FBI in 1995, 13 in 1996, 20 in 1997, and 17 in 1998. None of these cases resulted in prosecutions, yet FBI officials stated that in some instances Department employees admitted, when interviewed by FBI agents, the inappropriate and deliberate release of classified information to unauthorized individuals. In 1998 the Department reported 4 security violations (classified information was either actually released or possibly was compromised). These incidents resulted in 1 letter of reprimand, a 2 day suspension without pay, a 4-day suspension without pay, and a 30-day suspension without pay.

INR analysts frequently found instances where SCI was improperly handled and on occasion reported them to the INR security officer. The INR security officer stated that about once every 3 days there were instances of mishandled SCI. However, these cases were not forwarded to DS for adjudication. SCI incidents reported by INR analysts are followed up by INR staff who retrieve the missing SCI materials. Some examples include the following:

- SCI documents from NSA were not returned to SCIFs on numerous occasions.
- (b)(2)----------] pouch was returned without a highly classified document.
- The [(b)(2)---] pouch was not returned at the end of the day.
- The [(b)(2)----------]pouch was not returned to INR all weekend. When the pouch was returned to INR, it was empty.
- The [(b)(2)----------] pouch was open with the key in it when it was returned to the INR watch office.

Several Main State offices are selected randomly and inspected by the guard force after duty hours each day. Occasional Marine security guard inspections are performed as part of the

---

4. Contract security guard and Marine security guard after-hours security inspections were not performed for some time because of budget constraints in the Department. However, the after-hours security inspections were restarted in response to a GAO report.
5.The Intelligence Authorization Act of 1995, Section 811 (50 United States Code 402a) and Section 603 (28 United States Code 533), requires executive agencies or departments to report all indications that classified information is being or may have been disclosed in an unauthorized manner to a foreign government or an agent thereof to the FBI for prosecution.

guards' training for overseas inspections and are more thorough. Inspections by Marines resulted in an average of 63 security incidents identified during each of 8 inspections conducted in 1998.

Program Effectiveness

The security incident program is not effective because employee security awareness is lacking and administrative disciplinary actions have not been a sufficient deterrence.

Many employees cited for security incidents indicated that they were not aware of the procedures for handling and safeguarding classified materials. Bureau USOs were not reinforcing the need to protect classified material. In addition, DS officials reported that the Department's budget for briefing employees on required security practices has been significantly reduced in recent years.

The Department does not normally consider action against an employee until there are four security incidents within 18 months. If a serious incident occurs the Department may proceed with disciplinary action regardless of the number of incidents cited during the 18-month period. After the fourth incident, the deputy assistant secretary of DS sends a security warning letter to the employee. All subsequent incidents are referred to M/DGP for administrative action. Security violators may receive a letter of reprimand, be suspended without pay, or dismissed. There were 218 domestic and overseas employees with 4 or more security incidents during the 1 8-month period ending in September 1998. The OIG reviewed 40 of the 218 cases; 6 employees were suspended from 1 to 6 days, 10 received letters of reprimand, 16 received letters of warning, and 8 were not disciplined. None of the 218 employees was dismissed.

The security incident program has had little or no effect on employee clearance for access to SCI. Since August 1998, DS has forwarded the names of employees with SCI access and four or more security incidents in an 1 8-month period to INR security staff for possible revocation of SCI access. INR determined that such employees would lose access to SCI until they received a security briefing, after which their access would be restored, thus allowing repeat offenders to regain SCI access.

Classified information in the Department, including SCI, is vulnerable to compromise.

Recommendations

The OIG recommends that the Director General of Personnel:

8. Strengthen the disciplinary actions against employees for security incidents. [Action: M/DGP]

The OIG recommends that the Assistant Secretary of Diplomatic Security:

9. Increase the frequency of security briefings and related training afforded to employees. [Action: DS]

E UNIT SECURITY OFFICER PROGRAM

Many Unit Security Officers (USOs) were not performing their responsibilities to protect classified materials assigned to their organization in accordance with procedures prescribed in Department regulations. USO responsibilities were not performed because many USOs were not fully informed of their security responsibilities. Furthermore, USOs do not consider such duties a primary responsibility. USOs generally believed that they have no authority to enforce security procedures.

Criteria

The USO Program is required under 12 FAM 500. Bureau executive directors are responsible for ensuring bureaus have designated principal USOs. Each USO should maintain an active training and orientation program to inform employees of their responsibility for complying with the provisions of the security regulations. Supervisors or USOs should institute security checks before those conducted by security guards to ensure that classified material is properly stored and that containers are locked. To fulfill this requirement, supervisors must designate employees on a weekly basis to conduct after-hours security checks.

The Unit Security Officer Handbook issued by DS describes USO responsibilities including, but not limited to:

- Briefing new employees.
- Ensuring employees are appropriately cleared for the information to which they require access.
- Assigning escorts.
- Administering security measures for safeguarding classified and sensitive information, which include:
  - ✓ providing guidance on opening and closing security containers,
  - ✓ ensuring that close-of-business checkers have been designated by supervisors,
  - ✓ safeguarding combinations and ensuring that lock combinations are changed as required, and
  - ✓ establishing appropriate transmission, reproduction, and destruction procedures.
- Processing security incidents.
- Performing internal security reviews and other duties as necessary to protect sensitive and classified information.

USO Protection of Classified Information

USOs generally did not (1) institute internal security procedures such as a formal after-hours check system, (2) perform internal security reviews, or (3) brief employees routinely on security regulations. In 21 out of 23 offices, there were no assurances that after-hours check procedures were performed or that classified documents were properly stored. Of 23 USOs interviewed, 17 did not perform internal security reviews. The table below summarizes the USO program.

	[(b)(2) ------	------ ------	----- -----	----- ----	----- ----	----- -----
Total USO's interviewed at the Bureau	3	5	5	2	5	3
USO's believed that that they were adequately trained	1	1	2	0	5	3
USO's regularly briefed employees on security	1	2	2	0	4	2
USO's ensured that lock combinations are changed	0	0	1	1	0	0
USO's maintained safe combinations list	0	2	1	0	0	0
USO's processed security incident reports	3	5	4	2	2	1
USO's performed internal security review	0	1	0	1	4	0
USO's believed that USO training is adequate	0	1	1	0	4	2
Office instituted written security procedures	0	1	0	0	4	0
Office instituted after hours check	1	2	2	1	5	3
Office had tracking system to ensure that after hours are performed	0	0	1	0	1	0
Office escorted uncleared char force	0	0	1	0	3	1
Office escorted Maintenance and Repair personnel	1	2	2	1	4	2
All computers were labeled	3	2	4	2	5	3

USO Lack of Independence

Many USOs did not know their roles and responsibilities, such as administering security measures to protect classified and sensitive information, because no supervisor emphasized their USO responsibilities to them. In addition, many USOs did not receive training and orientation on Department security regulations. One USO requested training, but was told such training did not exist. One USO told the OIG "DS should remember that this [processing security incidents] is not our primary responsibility ...." Others believed that they were not empowered to enforce security procedures with their peers or more senior personnel.

In response to the "tweed coat" incident, DS assigned a full-time senior security officer to the Office of the Secretary, Executive Secretariat Staff (S/S-S) to:

- act as security officer and coordinator for all security issues and operations,
- plan and implement the full range of security briefings for all staff,
- supervise USOs and top secret inventory control officers in their security responsibilities,
- conduct investigations of security incidents and events as required, and
- ensure compliance with Diplomatic Security Service security practices and regulations in accordance with 12 FAM and E.O. 12958.

The on-site presence of a professional security officer has been well received by S personnel, and could be used as a model for other bureaus in the Department. Individuals from DS could assist Department offices and bureaus to establish appropriate internal security procedures and act as advisors to assistant secretaries and executive directors in implementing security policies.

Recommendations

The OIG recommends that the Assistant Secretary of Diplomatic Security:

10. Assign DS security personnel to headquarters regional bureaus as security advisors to establish and oversee internal office security procedures. [Action: DS]

11. Ensure that all USOs receive periodic training. [Action: DS]

LIST OF ABBREVIATIONS

CIA	Central Intelligence Agency
DCI	Director of Central Intelligence
DCID	Director of Central Intelligence directive
DS	Bureau of Diplomatic Security
E.O.	Executive Order
EUR	Bureau of European and Canadian Affairs
FAM	Foreign Affairs Manual
FBI	Federal Bureau of Investigation
INR	Bureau of Intelligence and Research
M/DGP	Bureau of Personnel
MDI	Monitor Dynamics, Inc.
NEA	Bureau of Near Eastern Affairs
NSA	National Security Agency
OIG	Office of Inspector General
PIN	Personal identification number
S	Office of the Secretary
SA	Bureau of South Asian Affairs
SCI	Sensitive compartmented information
SCIF	Sensitive compartmented information facility
SOIC	Senior official of the intelligence community
S/S-S	Office of the Secretary, Executive Secretariat Staff
SSCI	Senate Select Committee on Intelligence
TSWA	Temporary Secure Working Area
UL	Underwriters Laboratories
USO	Unit security officer

APPENDIX A
COMMENTS FROM THE BUREAU OF INTELLIGENCE AND RESEARCH

United States Department of State

Washington, D.C. 20520

July 21, 1999

UNCLASSIFIED

TO: OIG - Jacquelyn L. Williams-Bridgers

FROM: INR - Phyllis E. Oakley

SUBJECT: INR's Comments on OIG Report SIO/A-99-X

INR has read carefully the draft report entitled "Protecting Classified Documents at State Department Headquarters" and discussed the report with members of your staff. We understand that the last version we received will be issued without further changes.

As noted in the attached paper conveying our comments on the report and its recommendations, INR takes very seriously the observations of the auditors who performed the inspection and has already initiated steps to correct specific deficiencies. The audit revealed that we had a previously undiscovered problem in the Bureau security office and we acted immediately to correct the situation by replacing the [redacted]. We do not concur with the report's principal recommendation that responsibility for SCI materials be transferred from INR to DS. Our reasoning on this and other points made in the report is spelled out in the attached paper. (b)(6)

I request that INR's reply to this OIG report be included when the report is sent to Congress.

Attachment: As Stated.

cc: DS-DCarpenter

UNCLASSIFIED

APPENDIX A
COMMENTS FROM THE BUREAU OF INTELLIGENCE AND RESEARCH

INR Comments on OIG Report

The Bureau of Intelligence and Research welcomed the OIG audit (SIO A-99-X) of the Department's policies and procedures for handling classified information. We strongly agree with the report's core finding that it is both possible and necessary to enforce existing policies more rigorously, to tighten procedures, and thereby to reduce the danger of unauthorized disclosure of classified information. As specific deficiencies were called to our attention during the course of the inspection, we initiated remedial actions without awaiting the report's formal recommendations. INR has taken note of and viewed as constructive the report's critical observations and recommendations pertinent to INR's handling and protection of sensitive, compartmented information (SCI). The Bureau stands ready to cooperate with OIG and others to remedy any and all deficiencies.

INR cannot agree, however, with the OIG report's depiction of the Bureau's handling of SCI material, nor can INR concur in the recommendation that the INR Assistant Secretary delegate to DS the responsibility for protection of SCI material. INR also disagrees with the OIG report's characterization of the security requirements for briefing SCI materials outside of SCIFed offices when those materials remain continuously under the control of INR staff.

The report fails to distinguish clearly between Department-wide security deficiencies (which the report correctly [redacted] purview of DS) and INR's handling of SCI materials. The preponderance of security lapses and deficiencies examined by the auditors did not relate specifically to SCI materials. The result of the failure to draw an appropriately sharp distinction between the two categories of materials is to exaggerate the extent and severity of SCI-related problems. From evidence and judgments presented in the report, INR is seen to have discharged its security responsibilities for SCI materials more effectively than DS implemented Department-wide security regulations and procedures. Against this backdrop, we cannot understand or accept the logic by which OIG recommends shifting of INR's security responsibilities for SCI materials to the Bureau of Diplomatic Security.

We would draw particular attention to the following examples of imprecision or misunderstanding where the role of INR and the special nature of SCI materials are concerned.

- Section C, which deals with the Department's identification badge system, states: "The Department's current system does not meet DCID requirements on SCIF access control and makes unauthorized access to the building and to classified work areas feasible."

  - The Department of State is not a component of the Intelligence Community. The Department of State headquarters building is not a SCIF. INR, which is a part of

APPENDIX A
COMMENTS FROM THE BUREAU OF INTELLIGENCE AND RESEARCH

[redacted]

the intelligence community and has responsibility for control and storage of SCI material, is housed in fully accredited SCIFs with approved access controls.

[redacted] (b) (2)

- Section E correctly notes that "Once cleared to visit and issued a visitor's pass, most visitors move about the building unescorted."

- [redacted] (b) (2)

- This also implies, falsely, that an INR officer charged with briefing SCI materials in non-SCIFed space would proceed with such briefing upon entry of a visitor whose access and clearances were not known. To the contrary, the INR briefing officer retains all SCI materials under his/her personal control, and under standard procedures will cease the briefing until the access and clearances of the visitor could be ascertained.

INR feels strongly that the report should be redrafted using an organizational principle that draws the appropriate line of demarcation between the Department of State generally and INR, and between protection of ordinary classified information and SCI material. Thus, the audit should have first examined the situation pertinent to the headquarters building as a whole (i.e., a building that receives thousands of visitors, including foreign diplomats, journalists, and NGO representatives, who enter workspaces containing vast amounts of classified information, some of which is intelligence information). A security regime appropriate to this set of circumstances will need to rely heavily upon the diligence of the Department's employees. The unacceptably high incidence of security violations, as presented in the OIG's audit report, bespeaks a need for correction of the way in which the Department monitors visitors and trains and supports unit security officers.

The report ought next to have examined how SCI material is handled within that context. Most SCI materials never leave INR's approved SCIFs. Those which are briefed outside INR are conveyed via 46 pouches to Department principals such as the Secretary, the Under Secretaries, and selected Assistant Secretaries. INR agrees with the OIG report's determination that the offices of principals who receive pouches should be formally accredited as Temporary Secure Work Areas (TSWAs) in accordance with DCID requirements. SCI materials provided to Department principals in locked pouches are retained in TSWAs during normal working hours and must be returned to INR at close of business. INR does not, however, agree with the OIG report's determination that offices in which INR staff brief but do not leave SCI materials must be accredited as TSWAs. When INR staff bring SCI material to Department officers with the appropriate

APPENDIX A
COMMENTS FROM THE BUREAU OF INTELLIGENCE AND RESEARCH

[redacted]

clearances and need to know who do not work in the offices of Department principals who receive locked pouches, the INR staff remain with the materials at all times, thereby rendering irrelevant the question of whether the office has approved locks or other security features cited in the OIG report. [redacted] (b) (2)

The report's blurring of the essential distinction between overall security practices/lapses and those specific to SCI materials is also manifested in its summary statements intended to illustrate a major security problem: "The Department does not protect SCI information in accordance with DCID requirements" and "1,700 security infractions were issued at Main State in 1998; and SCI infractions were not pursued at Main State."

- The report notes that of the 1,700 infractions, only six involved SCI material. (For reasons unclear to us, this number increased from one to six between INR's meeting with the OIG team on June 9 and the publication of this draft. INR was not given information that would enable us to determine where/how controls had failed.

- The report observes, in a footnote, that of the 1,700 infractions, only four were deemed to be violations that *could* result in the actual or potential compromise of the material. The report does not state whether any of the violations involved SCI material, but INR was informed that they were referred to the Office of Personnel, not the FBI.

INR wishes to be very clear that even one infraction involving SCI material is unacceptable. The Bureau takes very seriously OIG's concerns about the way such materials are handled. We share OIG's view that it is essential to focus on the *potential* for compromise and hypothetical consequences of inadequate procedures, not simply on proven violations or adverse consequences. That having been said, INR has begun to work vigorously toward correcting the deficiencies cited by OIG.

The OIG Audit correctly states that the Bureau of Diplomatic Security (DS) is responsible for establishing and implementing policies for the protection of classified information, while by Executive Order and implementing directives the Assistant Secretary for Intelligence and Research, as a Senior Official of the Intelligence Community (SOIC), is responsible for the protection of SCI material. The report also notes correctly that the SOIC "may delegate responsibility for the implementation of policies and procedures defined in an appropriate DCID to a Cognizant Security Office." The report recommends that the SOIC should designate the Bureau of Diplomatic Security as its Cognizant Security Office.

The rationale advanced in support of this key recommendation is not persuasive.

APPENDIX A
COMMENTS FROM THE BUREAU OF INTELLIGENCE AND RESEARCH

[redacted]

- The recommendation would place security responsibility outside the direct control of the SOIC, violating fundamental principles of good management. We would further note that DS faces significant staffing shortfalls, and is already strained to perform its mandated responsibilities.

  In any case, INR has moved quickly to address this situation as described by OIG.

- It granted an early release to the [redacted] and converted that Foreign Service position to Civil Service. The new position reports directly to the SOIC through an internal INR chain of command. (b) (6)

- A [redacted] security officer of proven ability and managerial experience was identified, recruited, and brought to INR effective July 6. That officer has the active support of Bureau management. We are confident that he will provide the necessary leadership, technical skills, and dedication to improve the protection afforded sensitive compartmented information. (b) (6)

- The security section recently initiated annual security awareness refresher briefings for all Department personnel who hold SCI clearances, and has reviewed SCI handling procedures to ensure that they are fully understood by all who handle such materials.

- To correct for the [redacted] failure to perform update inspections of TSWAs used by Department principals for the temporary storage of SCI materials, INR's [redacted] immediately initiated such inspections and prepared the requisite paperwork. To date, eight have been re-inspected and accredited. (b) (6) (b) (2)

- To ensure that pouches are always returned to INR at close of business, the security chief is implementing new procedures requiring that the INR Watch call the person who has signed for any pouch not returned by a specified time. When appropriate, security violations will be issued.

- The Bureau has requested an additional security officer position in its 2001 budget request. The additional officer will enable the Bureau to enhance further its security efforts.

Additional Comments

In addition to the major areas of disagreement noted above, INR believes it important to respond for the record to a number of specific points made in the OIG report which we believe to be misleading mischaracterizations of the situations they purport to describe. The order of these comments corresponds to the sequence in which the characterizations appear in the OIG report.

APPENDIX A
COMMENTS FROM THE BUREAU OF INTELLIGENCE AND RESEARCH

[redacted]

-4-

- Pages 3-4 of the report states that tension between intelligence producers and policymakers creates an environment within the Department that places less emphasis on safeguarding information than is the case in other national security and intelligence organizations. This paragraph misconstrues the very real tension that exists between the need to protect sources and methods and the wish to use what is learned through intelligence to protect US foreign policy and security interests. That tension is manifest in the almost daily exchanges between policymakers and intelligence collectors to reach agreement on the language that can (and cannot) be used in diplomatic demarches. Those battles are fought daily, and the results are honored by policymakers. The existence of this inherent tension—which also exists in other agencies where policy decisions are informed by covertly obtained information—does not, as the OIG report asserts, cause the Department of State or its personnel to be less attentive to the need to safeguard classified information than are other national security organizations. No empirical evidence is provided to justify this sweeping, and we believe unjustified, assertion.

- Pages 6-7 focuses on the briefing of SCI material in offices that have not been inspected and accredited as SCIFs or TSWAs and lack [redacted] and other requirements needed to qualify for such accreditation. INR maintains, and the CMS office responsible for the DCIDs agrees, that the DCIDs do not require such accreditation if SCI materials remain constantly in the physical possession of INR officers who ensure that they are seen only by persons with the requisite clearances and need to know. (b) (

- Page 8 contains a paragraph dealing with hardcopy NSA products provided through the Cryptological Services Group (CSG) integrated into the INR Watch. That paragraph states that the OIG review determined that 12.5 percent of the documents sent to [redacted] had not been returned to the CSG at the time the inspection was performed—leaving the impression that this demonstrated improper handling of these SCI materials. This OIG statistic is meaningless and bears no relationship to proper security procedures. All special hardcopy NSA documents must be returned to the CSG for ultimate disposition, but there is no limit as to the amount of time they can be held in a properly accredited SCIF. The INR front office informed the OIG auditor that instructions printed on the cover sheet of NSA documents specify that they are to be returned to the INR front office, and that the "missing" documents almost certainly were in the stack of returned materials in the INR front office SCIF (in the safe of the Special Assistant who collected the materials and returned them in batches to the CSG). This fact was called to the attention of the OIG on three occasions – before the report was drafted, after the first draft was shared with INR, and after the current draft was produced. Our new security chief has reviewed the situation with the CSG liaison officer who opined that although better accountability might be achieved if there were fewer operational and staffing constraints, her overall (b) (

APPENDIX A
COMMENTS FROM THE BUREAU OF INTELLIGENCE AND RESEARCH

[redacted]

assessment is that all CSG documents are well protected, even when not returned promptly.

- Page 9 of the report describes INR's principal mission (as defined by the OIG) and states that the Bureau assigns lower priority to security requirements than to the timely distribution of information. A more accurate characterization—provided to the OIG in written form after receipt of the initial draft—is:

  - INR's principal mission is to ensure that Department principals and operational officers receive timely delivery of all source intelligence and analysis germane to their areas of responsibility and in accordance with their security clearances and need to know. INR management relies on the integrity and security awareness of the principals and senior staff entrusted with temporary custody of SCI materials. Adherence to security requirements is not a lower priority.

- On page 9, the report states that INR's security office has not been providing the requisite management of SCI materials and that INR and DS security personnel are aware of improper handling of classified material. One of the immediate benefits of this OIG audit was to bring to the attention of the INR front office possible security problems that the incumbent head of the Bureau's security office had failed to report to the SOIC or PDAS. What the OIG auditors were told appeared, in a number of cases, to be different from what he had told the SOIC and PDAS about INR's procedures. INR did not wait for the formal OIG report to take action. The officer was allowed to depart for another assignment before his normal rotation date, the position of security office director that had been filled by a series of DS officers was returned to the Bureau of Diplomatic Security, and a career security officer was recruited from USIA to correct deficiencies identified by the OIG.

- [redacted] (b)(2)

[redacted]

7

- Page 16 lists a number of examples to show that the Security Incident Program is not effective in preventing security incidents, all of which refer to the handling of SCI materials. Unfortunately, the report—and the OIG—provided insufficient information to determine the magnitude or locus of the problem to permit remedial action. For example, the statement that NSA documents were not returned to SCIFs on numerous occasions is not very helpful because it includes cases where pouches that were not returned until INR staff retrieved them from the cognizant officer in the TSWA after normal close of business as well as the special NSA documents "not returned to CSG" noted above. At least some of these incidents seem to have been reported to the OIG auditors by the [redacted] who kept no records and did not report the incidents to the SOIC or the PDAS. Proper procedures may not always have been followed, but we have no means to establish the veracity of what that officer alleged to the OIG—information that does not correspond to what he told the SOIC and/or PDAS. Noting that the [redacted] pouch did not come back at the end of the day probably is true, but the contents of [redacted] pouch sometimes are returned to the INR special assistant during the day and the pouch may not have been returned because at the end of the day it contained no SCI. Moreover, the first action of responsible INR Watch officers upon discovery that a pouch has not been returned is to inquire about its whereabouts and, if necessary, to retrieve it. That practice is now being codified in a formal INR policy. (b)(6 (b)(2 (b)(2 (b)(2

7