Description of document:	Department of State (DOS) Inspector General (OIG) Protection of Classified Information of State Department Headquarters, 2005
Requested date:	25-March-2009
Released on appeal:	22-May-2025
Posted date:	28-July-2025
Source of document:	FOIA Officer Office of General Counsel Office of Inspector General U.S. Department of State 1700 North Moore Street, Suite 1400 Arlington, VA 22209 Fax: (202) 261-8579 Email: FOIA@stateoig.gov FOIA.gov

Office of Inspector General
United States Department of State

May 22, 2025

SENT VIA EMAIL

Subject: Department of State, Office of Inspector General Freedom of Information Act Appeal

This is in response to your appeal of the response to your Freedom of Information Act (FOIA) request to the Department of State (DOS), Office of Inspector General (OIG), which you originally filed with the Department of State, Office of Information Programs and Services (IPS) on March 25, 2009.

In November 2023, the responsibility for handling FOIA appeals related to OIG FOIA requests moved from IPS to OIG's Office of General Counsel. During this transfer of responsibility, OIG learned that IPS had several pending appeals, many of which were years old. Unfortunately, your appeal was among those still pending.

Your FOIA request for OIG report SIO-A-05-13 was originally withheld in full because the report was classified. Upon further review, OIG consulted with the Department of State and can now release a redacted version of the report to you. As such, we are providing you:

9 pages are released in full;
42 pages are released in part;
4 pages are withheld in full.

These redactions were made pursuant to Exemptions 1, 5, 6, and 7 of the FOIA further discussed below.

Exemption 1, 5 U.S.C. § 552(b)(1)

Exemption 1 of the FOIA protects information that has been deemed classified "under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy" and is "in fact properly classified pursuant to such Executive order." 5 U.S.C. § 552(b)(1). DOS-OIG is invoking Exemption 1 to protect information classified by the Department of State.

Exemption 5, 5 U.S.C. § 552(b)(5)

Exemption 5 of the FOIA protects "inter-agency or intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency." 5 U.S.C. § 552(b)(5). DOS-OIG is invoking the deliberative process privilege of Exemption 5 to protect information that falls within that privilege's domain.

Exemption 6, 5 U.S.C. § 552(b)(6)

Exemption 6 allows withholding of "personnel and medical files and *similar files* the disclosure of which would constitute a clearly unwarranted invasion of personal privacy." 5 U.S.C. § 552(b)(6) (emphasis added). DOS-OIG is invoking Exemption 6 to protect the names of lower-level employees and any information that could reasonably be expected to identify such individuals.

Exemption 7(E), 5 U.S.C. § 552(b)(7)(E)

Exemption 7(E) protects all law enforcement information that "would disclose techniques and procedures for law enforcement investigation or prosecution or would disclose guidelines for law enforcement investigations or prosecution if such disclosure could reasonably be expected to risk circumvention of the law." 5 U.S.C. § 552(b)(7)(E). DOS-OIG is withholding from disclosure specific information which could reasonably be expected to risk circumvention of the law.

Dispute Resolution Services

In 2007, the Office of Government Information Services (OGIS) was created to offer mediation services to resolve disputes between FOIA requesters and Federal agencies as a non-exclusive alternative to litigation. Using OGIS services does not affect your right to pursue litigation. You may contact OGIS at ogis@nara.gov, by telephone at 202-741-5770 or toll free at 1-877-684-6448, by facsimile at 202-741-5769, or by mail at: Office of Government Information Services, National Archives and Records Administration, 8601 Adelphi Road-OGIS, College Park, MD 20740-6001.

This represents DOS OIG's final determination and exhausts all administrative remedies available to you. As you may know, you have the right to seek judicial review of this determination under 5 U.S.C. § 552(a)(4).

Sincerely,

Jeffrey McDermott

Digitally signed by Jeffrey McDermott
Date: 2025.05.22 09:57:00 -04'00'

Jeffrey McDermott
Assistant Inspector General

~~CONFIDENTIAL~~

United States Department of State
and the Broadcasting Board of Governors
Office of Inspector General

Security and Intelligence Oversight Audit

Protection of Classified Information at State Department Headquarters

Report Number SIO-A-05-13, February 2005

IMPORTANT NOTICE

(U) CLASSIFICATION: The information contained in this report is classified SECRET/NOFORN and is intended solely for the official use of the Department of State or the Broadcasting Board of Governors. No secondary distribution may be made, in whole or in part, outside the Department of State or the Broadcasting Board of Governors, by them or by other agencies or organizations, without prior authorization by the Inspector General. Public availability of this document will be determined by the Inspector General under the U.S. Code 5 U.S.C. 552. Improper disclosure of this report may result in criminal, civil, or administrative penalties.

Classified by: Cameron R. Hume
Deputy Inspector General
REASON: 1.4(g)

~~CONFIDENTIAL~~

OFFICE OF INSPECTOR GENERAL
OFFICE OF SECURITY AND INTELLIGENCE OVERSIGHT

PROTECTION OF CLASSIFIED INFORMATION AT STATE DEPARTMENT HEADQUARTERS (SIO/A-05-13)

EXECUTIVE SUMMARY (U)

(U) Section 832 of the Intelligence Authorization Act of 2003 (Public Law 107-306) directs the Office of Inspector General (OIG) to conduct annual evaluations of the Department's policies and procedures for protecting classified information at its headquarters for the 2002, 2003, and 2004 calendar years. OIG is also required to review the Department's compliance with Director of Central Intelligence Directives (DCIDs) regarding the storage and handling of Sensitive Compartmented Information (SCI) material.

(U) Based on an agreement between staffs of the U.S. Senate Select Committee on Intelligence, the U.S. House of Representatives Permanent Select Committee on Intelligence, the DCI's Special Security Center, and OIG, the 2004 evaluation focused on the Department's compliance with DCIDs involving Personnel Eligibility for SCI Access (DCIDs 6/4 and 1/20P) and Protecting SCI Within Information Systems (DCID 6/3). OIG was also requested to provide updated information on issues included in its 2003 report, which focused on SCI document accountability and control (DCID 6/1), physical security (DCID 6/9), and the Department's system for tracking security violations committed by its employees.

SCI PERSONNEL SECURITY (U)

(U) The Department meets the DCID 6/4 requirements for Personnel Security. Because of the effective working relationships among the many offices involved, requests for SCI access are processed and granted efficiently. OIG tested the Department's management of SCI access, including the initial requests for access, the processes used to grant SCI access, the indoctrination-briefing program, the periodic security awareness and education program, and the process of removing names from the SCI access roster for individuals no longer requiring SCI access due to employment transfers and terminations. OIG sampled the Department's records for 60 individuals, including employees, contractors, detailees, and retired annuitants, for whom SCI access was requested during a one-year period. OIG found that the Department properly investigated the candidates' backgrounds, provided indoctrination briefings, provided security awareness and education trainings, and debriefed individuals who no longer needed SCI access. Although the processes to grant and terminate SCI access met DCID requirements in all material respects, OIG recommended that the Department strengthen

its filing system for background investigations to ensure that the files contain updated and complete information.

DCID REQUIREMENTS – PERSONNEL ASSIGNMENTS AND TRAVEL (U)

(U) The Department's policies and procedures effectively enable SCI-indoctrinated personnel to meet DCID requirements concerning travel or assignment to hazardous countries. These policies and procedures advise SCI-indoctrinated individuals regarding requirements to report official and unofficial foreign travel and how to obtain necessary defensive security briefings. Although they are effective, the procedures could be improved by consolidating employee travel-reporting requirements into one DS office. Additionally, the Department should monitor the status of DCID 6/10, which is in draft and will replace DCID 1/20(P). It should amend Department policies or procedures as needed when the new DCID is issued.

SCI AUTOMATED INFORMATION SYSTEMS (U)

(SBU) The Department's policies and procedures comply with DCID 6/3 requirements for protecting SCI material within automated information systems. In addition, the Bureau of Intelligence and Research (INR) and the Bureau of Diplomatic Security (DS) are effectively addressing their respective responsibilities. Furthermore, directives developed by DS, are facilitating implementation of the DCID's requirements, although opportunities exist to improve program management. [redacted]

STATUS OF ISSUES IDENTIFIED IN OIG's 2003 REPORT

(U) OIG in its report for the 2003 audit (SIO-A-04-11), reported that the Department met DCID requirements for SCI handling and control (DCID 6/1) and physical security (DCID 6/9). However, the report recommended procedural changes to improve DCID implementation. OIG followed up on those recommendations during its 2004 review and found that the Department has implemented the recommended changes for improving control of both *accountable* and *non-accountable* SCI material and has strengthened its procedures regarding SCI physical security.

(U) OIG's 2003 audit also said the Department has developed and implemented a system to track employee security violations but OIG found [redacted]

AGENCY COMMENTS (U)

(U) DS reviewed and provided a written response to a draft version of this report. The bureau concurred with all of the report recommendations that are addressed to DS.

(U) INR reviewed a draft version of this report and provided a written response. The bureau concurred with all of the report recommendations that are addressed to INR.

(U) HR reviewed a draft version of this report and informed OIG that it plans to [redacted] (SBU)

(U) Specific DS, HR and INR comments have been incorporated into the body of the report where appropriate. The comments for INR and DS are included in their entirety in the report's Appendices A and B, respectively.

OFFICE OF INSPECTOR GENERAL
OFFICE OF SECURITY AND INTELLIGENCE OVERSIGHT

PROTECTION OF CLASSIFIED INFORMATION AT STATE DEPARTMENT HEADQUARTERS

TABLE OF CONTENTS (U)

EXECUTIVE SUMMARY i

PURPOSE AND SCOPE 1

BACKGROUND 3

FINDINGS 4

A. Personnel Security Eligibility 4

B. Automated Information Systems 21

C. Document Control 30

D. SCI Physical Security 33

E. [redacted] 34

RECOMMENDATIONS 36

ABBREVIATIONS 38

APPENDIXA – INR Comments X

APPENDIX B – DS Comments X

PURPOSE AND SCOPE (U)

(U) This review responds to the third and final annual requirement for Section 832 of the Intelligence Authorization Act of 2003, which required OIG to evaluate State Department compliance with the DCIDs pertaining to the storage and handling of SCI material at its headquarters. OIG addressed the first and second annual requirements in February 2003 and February 2004 by providing Congress with reports titled, Status Report – Protection of Classified Documents at State Department Headquarters and Protection of Classified Information at State Department Headquarters, respectively. In the 2003 report, OIG noted that DS had made substantial improvements in the protection of classified information, particularly SCI material, since 1998. Based on an agreement between staffs of the U.S. Senate Select Committee on Intelligence, the U.S. House of Representatives Permanent Select Committee on Intelligence, the DCI's Special Security Center, and OIG, the 2004 evaluation focused on the Department's compliance with DCIDs involving Personnel Eligibility for SCI Access (DCIDs 6/4 and 1/20P) and Protecting SCI Within Information Systems (DCID 6/3). OIG was also requested to provide updated information on issues included in its 2003 report, which focused on SCI document accountability and control (DCID 6/1), physical security (DCID 6/9), and the Department's system for tracking security violations committed by its employees.

(U) OIG concluded in the 2003 report that the Department's methods for maintaining accountability and control of SCI documents, that are categorized as *accountable* and *non-accountable*, comply with DCID 6/1 requirements. OIG found that, although the Department has instituted strict procedures for receiving, recording, transferring, and destroying these documents, [redacted]. OIG also concluded that the Department employs an effective process for accrediting sensitive compartmented information facilities (SCIFs) according to DCID requirements. Lastly, OIG found that the Department had developed and implemented a system to track employees' security violations. However, OIG recommended [redacted]

(U) To meet the Act's third annual requirement, which pertains to calendar year 2004 activity, and to ensure that the recommendations of its 2003 report were correctly implemented, OIG consulted with the DCI Special Security Center's Controlled Access Program Coordination Office (DCI/SSC/CAPCO) and with the DCI's Chief Information Officer's staff, to ensure the Department's compliance with DCIDs 6/3, 6/4, and 1/20P. OIG and the DCI agreed to review these issues in the project plan that they jointly developed in 2003 . The 2004 calendar year review focused on personnel security

[1] In 2003, OIG and DCI/SSC/CAPCO agreed to a project plan focusing on SCI Document Control and Accountability (DCID 6/1), Personnel Security (DCIDs 6/4 and 1/20P), Automated Information Systems (DCID 6/3), and Physical Security Standards (DCID 6/9).

(DCIDs 6/4 and 1/20P) and automated information systems' (DCID 6/3) security, and followed-up on issues raised in the 2003 review.

(U) The 2004 review focused on whether the Department controls personnel access to SCI material according to DCID 6/4 and other federal regulations and whether the Department controls the automated information systems used to process SCI material according to DCID 6/3 and other federal regulations. To assess personnel security, OIG interviewed officials in DS's Special Security Office (DS/SSO), Office of Personnel Security/Suitability (DS/PSS), Industrial Security Division (DS/IND), HR, and INR. OIG confirmed through sampling that DS, HR, and INR policies and procedures have been implemented.

(U) To assess automated information systems security measures, OIG interviewed officials in DS and INR [redacted] to provide advice concerning DCID requirements. OIG reviewed policies and procedures addressing the certification and accreditation of automated information processing equipment and reviewed Department guidance that implements DCID 6/3. OIG also reviewed available systems documentation, including the systems security plan, contingency plan, and certification and accreditation manual, and reviewed the [redacted] To determine the requirements for protecting SCI information, OIG reviewed DCID 6/3. OIG also reviewed the Department's supplemental guidance, DS's Sensitive Compartmented Information Systems Standards, Concept of Operations and Standard Operating Procedures, to ensure all DCID 6/3 requirements were addressed.

(U) To determine automated information systems' compliance with applicable documentation, OIG reviewed available systems documentation, including the systems security plan, contingency plan, and certification and accreditation manual. To determine the validity of the certification and accreditation process, the OIG reviewed [redacted] used by DS for assessing the vulnerabilities of the INR's SCI system, and compared it with DCID 6/3. These procedures were supplemented by interviews with officials in INR and DS.

(U) The review was conducted in accordance with generally accepted government auditing standards by OIG's Office of Security and Intelligence Oversight and its Office of Information Technology. The review of the Department's compliance with DCIDs 6/4 and 1/20P and the assessment of issues arising from OIG's prior report (DCIDs 6/1 and 6/9 and the Department's system for tracking security violations) was conducted by Audit Manager [redacted] and Senior Auditors [redacted] and [redacted] The review of the Department's compliance with DCID 6/3 was conducted by Deputy Assistant Inspector General for Information Technology [redacted] and Senior Auditor [redacted]. Fieldwork was conducted in Washington, D.C., from April 8 through September 15, 2004.

BACKGROUND (U)

(U) OIG has reviewed the Department's programs for protecting classified information since 1998 and has issued seven reports[2] addressing the strengths, weaknesses, and improvements in the Department's handling and control of classified information. Since the initial report in 1998, when OIG reported that the Department was substantially not in compliance with DCID requirements for handling SCI material, the Department has accredited and certified SCIFs, developed and implemented procedures for closely tracking and controlling classified material, improved its protection of SCI within information systems, and improved its security awareness and security incident programs.

(U) In its report, Protection of Classified Information at State Department Headquarters, dated February 2004, OIG reported that the Department's methods for maintaining accountability and control of SCI documents, categorized as *accountable* and *non-accountable*, complied with DCID requirements and that the Department employed an effective process for accrediting SCIFs according to DCID requirements. Additionally, OIG confirmed that the Department had developed and implemented a system to track employees' security violations. OIG recommended [redacted] The Department addressed the recommendations and OIG followed-up on the implementation during the 2004 review.

[2]Management of SCI Access, SIO/A-98-49; Protecting Classified Documents at State Department Headquarters, SIO/A-99-46; Enhancing the Protection of Classified Material at State Department Headquarters, SIO/A-02-35; Status Report – Protection of Classified Documents at State Department Headquarters, SIO/A-03-30; Unit Security Officer Program, SIO/SPA-03-35; Protection of Classified Information at State Department Headquarters, SIO/04-11; Protection of Classified Information Overseas, SIO/A-04-08.

FINDINGS AND RECOMMENDATIONS (U)

A. PERSONNEL SECURITY ELIGIBILITY (U)

PERSONNEL SUITABILITY CONTROLS (U)

(U) The Department's procedures for granting SCI access to personnel, from the initial request for SCI access to the final granting of access, are an effective method of meeting DCID requirements and other applicable control procedures. OIG found that the Department's process to grant SCI access is thorough, proper, and effective. Through observation, examination, and detailed testing, OIG found that DS properly checks available background security files to determine each individual's eligibility for SCI access. However, OIG found [redacted] OIG made informal recommendations addressing these issues because it did not find them materially affecting the process of granting SCI access.

Requirements (U)

DCID Requirements (U)

(U) DCID 6/4 requirements for granting SCI access apply to all persons regardless of civilian or military status, form of employment, official rank or position, or length of service.[3] The "need to know" principle governs the granting of access, in accordance with personnel security standards and procedures, meaning that a possessor of classified information has determined that, in the interest of national security, a prospective recipient requires access to, knowledge, or possession of classified material to fulfill essential job requirements. The following criteria determine "need to know" for SCI access:

- The individual requesting access must be a U.S. citizen;
- The individual's immediate family members must be U.S. citizens;
- Members of the individual's immediate family or persons with whom they are bound to by affection or obligation must not be subject to physical, mental, or other forms of duress by a foreign power, persons engaged in criminal activity, or those who advocate the use of force to overthrow the U.S. government; and
- The individual must be stable, trustworthy, reliable, of excellent character, judgment, and discretion, and of unquestioned loyalty to the United States.

[3] The requirements do not apply to elected officials of the U.S. government, federal judges, and those individuals for whom the DCI makes a specific exception.

(U) The DCID permits exceptions to the personnel security standards, using a common-sense determination that the specific risk to national security is manageable. The Senior Official of the Intelligence Community (SOIC) may grant exceptions to the criterion of citizenship for an individual's family members or that dealing with those bound to the individual by affection or obligation, but only the DCI may grant an exception to the criterion that the individual requesting SCI access be a U.S. citizen. The individual must obtain a certification from his/her office describing a "compelling need" for SCI access, when the exceptions are granted for individuals and their immediate family members.

(U) The DCID requires that each individual nominated for SCI access have a completed Single-Scope Background Investigation (SSBI) and that the agency granting the clearance conduct investigations for certain family members under specific circumstances. Also, if an employee has an SSBI that has been completed within the last five years, the SSBI may serve as a basis for granting approval, unless information shows that the employee would not meet the adjudicative guidelines of the DCID. Periodic reinvestigations must be completed, if the SSBI is outdated, and thorough investigations are performed if the individual has lived outside of the United States for a substantial period of time. Additionally, the DCID authorizes the Determination Authority (DA) to accept an SSBI that is no more than six months beyond the five-year periodic reinvestigation.

(U) The SOIC may grant temporary SCI access before the SSBI is completed if it is in the interests of national security. The temporary clearance is accepted only at the agency for which it was approved or other agencies choosing to accept it. The temporary clearance permits the individual to perform only authorized functions, and the granting agency must modify its indoctrination briefings to ensure that only certain SCI information is presented.

(U) Trained professional DS/PSS adjudicators, who are under the cognizance of the SOIC, evaluate the information necessary to determine an individual's eligibility for SCI access. The DA makes the decision to grant SCI access based upon the DS/PSS adjudicator's recommendation. Any doubts about an individual that arise during the SCI access process must be resolved in favor of national security. The DCID also identifies appeals procedures for individuals to use when SCI access has been denied or revoked.

Other Requirements (U)

(U) Certain government-wide regulations govern access to classified information, including SCI material. Executive Order 12968 governs access to classified information and states that no employee shall be granted access to classified information unless that employee is eligible based upon a favorable adjudication of an appropriate background investigation, has a demonstrated need to know, and has signed an approved DCI-authorized SCI Non-disclosure Agreement (NdA). Additionally, National Security Directive 63 directs that all agencies and departments granting access to Collateral Top

Secret/National Security Information and SCI material must perform background investigations for employees in the Executive Branch.

~~(SBU)~~ According to 12 FAM 231.2, Security Authority, the Secretary of State has the right to suspend the employment of any officer or employee of the Department if such action is necessary to national security. Additionally, the regulation refers to the DCIDs that provide additional standards and procedures governing eligibility for access to SCI material.

~~(SBU)~~ Furthermore, 12 FAH-4 H-500 governs the Department's background investigations process and states that an SSBI is required for access to SCI material and collateral Top Secret information. Additionally, periodic updates should be conducted every five years to determine continued security-clearance eligibility for persons with Secret or Top Secret clearances.

SCI Access Procedures (U)

Initial Request for SCI Access (U)

(U) When a domestically stationed employee, contractor, or retiree in WAE[4] status, needs access to SCI material the executive officer should send a memorandum to INR's DA, through DS/SSO, requesting SCI access for the individual. If the employee is assigned to an overseas post, the deputy chief of mission, the post's Regional Security Officer, or the regional bureau executive officer sends the information to INR through DS/SSO via a telegram, e-mail or memorandum. The individual must have a current security clearance and a demonstrated need to know that the requesting bureau, office, or overseas post must justify.

(U) On receipt, DS/SSO reviews the memorandum, e-mail or telegram containing the individual's name, Social Security number, date and place of birth, federal pay grade, office symbol, position title, assignment dates, and telephone number as well as the onward assignment of the employee that the individual is replacing (if applicable) and the justification for SCI access. DS/SSO creates a file and enters pertinent information for employees, retirees, and contractors into its database. During a majority of the review fieldwork, DS/SSO used a Microsoft Access-based database to hold this information, but it now uses a new catabase, [redacted] DS/SSO is transferring the data from the Microsoft Access database into [redacted] Once indoctrinated, [redacted]

(U) After entering the information into the databases, DS/SSO fills out a form called a Diplomatic Security Letter (DSL), which it sends to DS/PSS. DS/PSS uses the DSL to

[4] WAE means, "when actually employed," as defined in 3 FAM 7413.1, and is employment of retired individuals on an irregular or occasional basis where hours or days of work are not normally based on a prearranged schedule.

begin the process to determine the person's eligibility for SCI access, as explained below. The DSL includes the subject's name, Social Security number, pay grade, and bureau/office symbol or post name.

Process to Send Information to DS/PSS (U)

(U) DS/SSO sends the completed DSL form to DS/PSS to determine whether the individual is eligible for SCI access based on security clearance information that DS/PSS maintains. DS/PSS performs background investigations for individual security clearances and reviews personnel security clearance files to determine eligibility. After DS/PSS receives the DSL and assigns the file to an adjudicator, the adjudicator searches the PSS Case Management System (CMS) database it maintains, to determine the status of the person's clearance and whether the subject has had SCI access in the past. If the Department issued the clearance, CMS would contain the individual's security clearance information. If PSS is unable to find the clearance information, it notifies DS/SSO, who contacts the requesting bureau so that it can verify whether another agency issued the clearance for a contractor, frequent visitor, or detailee. The DS Industrial Security Branch (DS/IND) and the DS/PSS Certification Unit use [redacted] database to track visitors, detailees, and contractors and annotate their security clearance status and SCI access levels. The DS/PSS Operations Support Branch receives requests for new employee security clearances and creates file folders for the individuals. Once the file exists, the DS/PSS Operations Support Branch conducts National Crime Information Center database checks, national agency checks, Defense Clearance and Investigations Index checks, and reviews credit reports. The DS/PSS Operations Support Branch enters the file and results of the background checks into CMS and then informs the adjudication branch in DS/PSS that the files are ready for further review.

(U) For current Department employees who already have a security clearance, the DS/PSS Operations Support Branch runs the aforementioned checks and forwards the DSL to the DSS/PSS adjudication branch, where one of two adjudicators dedicated solely to processing SCI access requests reviews the pertinent security clearance information. If the individual is an employee or WAE, the request remains in DS/PSS for adjudication, but if the individual is a contractor, the request is sent to DS/IND for separate processing and then to DS/PSS.

Employees/WAEs

(U) For SCI access requests for employees and WAEs, the team leader in DS/PSS assigns an adjudicator to the file. The adjudicator searches the CMS database for the subject's name and electronically requests his/her security clearance file from the DS/PSS file room. The adjudicator reviews the file and determines whether the person's security clearance information is current and whether the individual has outstanding issues that may affect his/her eligibility for SCI access. The adjudicator makes notes while reviewing the file and determines whether the issues have been resolved. For example, if the adjudicator notes that

members of the individual's immediate family are not U.S. citizens, he will ensure that appropriate follow-up procedures have been instituted.

(U) If the adjudicator needs specific follow-up work completed, he/she will send a tasking memorandum to either the individual or the Periodic Reinvestigation element of PSS that will initiate a background check for contacts such as immediate family members. The individual or Periodic Reinvestigation element adjudicator sends the memorandum to a DS field office or an overseas post, which follows-up and provides a report to the adjudicator. If the adjudicator determines that the foreign-connection issue was not adequately resolved, only the SOIC or DA can resolve it by waiver. Therefore, the adjudicator would state that the individual may not be eligible for SCI access and the DA must decide whether or not to grant SCI access.

Detailees (U)

(U) If a detailee requires SCI access, the special security officer of the individual's parent agency will coordinate with the special security officer of the detailee's assigned office to either verify the individual's SCI access or to grant it. According to DCID 6/4, within the Intelligence Community and subject to certain conditions, a favorable DCID eligibility determination for access to SCI made by one adjudicative authority under the SOIC is a favorable determination for all SOICs. The individual must also have a need-to-know in order to determine reciprocity of SCI access.

Contractors (U)

(U) Contract requirements dictate which contractors need SCI access. The bureau personnel then send the request on a DD 254 form to DS/IND, which forwards a copy of the DD 254 with a generic initial security clearance package to the contractor's facilities security officer. The facilities security officer ensures that the package is properly completed and sends it back to DS/IND. DS/IND fills out a DSL and a request for security clearance form (DS 1143) and sends the forms to DS/PSS for clearance adjudication and SCI access eligibility.

(U) Next, DS/PSS requests the contractor's investigative file from the agency that performed the background investigation for the contractor's security clearance. The agency determines whether the individual has a current security clearance and verifies this by sending a letter of consent to the facilities security officer of the contracting company, informing it of the status of the security clearance. The facilities security officer determines whether the contractor needs a new or updated security clearance, and then sends a visit-request letter and a letter of consent to the contractor. The background investigation for the existing security clearance must have been conducted within the past five years; otherwise, it is considered to be out of scope and the contractor will not be considered eligible for SCI access until a new investigation has been initiated and preliminary

checks have been conducted. DS/IND uses the [redacted] track visitors, detailees and contractors and annotate their security clearance status and SCI access levels. Next, the facilities security officer sends the completed package to DS/IND, which forwards it to DS/PSS. DS/PSS reviews the package, including the investigative file, determines whether the person is eligible for SCI access, and makes a recommendation for SCI access on the DSL, which it sends it through DS/SSO to the DA for final approval or denial.

(U) After the DA has granted or denied access, the DA advises DS/SSO and it informs the requesting bureau official, DS/PSS and DS/IND of the decision on SCI access. The bureau notifies the contracting company's facilities security officer. DS/SSO then schedules the date of the indoctrination briefing for the contractors who have been granted SCI access. After the contractor has received the indoctrination briefing, he or she may begin working under the contract.

(U) DS/IND and DS/PSS retain copies of the decision memorandum that DS/SSO provides to the requesting bureau, although there is no DCID requirement that DS/SSO keep the file indefinitely. (DS/SSO must retain the NdA for 70 years.)

INR Determination Authority (U)

(U) As specified in DCID 6/4.10, the incumbent DA is [redacted] the SOIC. He has the authority to grant, deny, suspend, or revoke SCI access to Department employees, WAEs, contractors, or others considered Department employees.

General (U)

(U) Generally, if DS/PSS recommends granting SCI access, the DA will grant it. If DS/PSS recommends that a person should not have SCI access, the DA normally reaches a similar conclusion, but only after independently reviewing files maintained by DS/PSS, DS Office of Investigations and Counterintelligence, Counterintelligence Division (DS/ICI/CI), or other applicable record holders. When DS/PSS recommends that the person may be eligible for SCI access, the DA may attempt to resolve outstanding issues through personally interviewing the individual, requesting that the individual bring in documentation of citizenship or proof of satisfaction of financial obligations, conducting an in-depth review of the individual's security clearance file, or by otherwise developing sufficient information about the individual to determine his or her suitability for SCI access.

Granting of SCI Access (U)

(U) If the DA agrees with the initial DS recommendation for eligibility, then that official will grant the SCI access and provide a memorandum to DS/SSO. SCI access is granted in one of four categories: unconditionally, waivered as to

standards, temporary (rarely granted) pending completion of a background investigation and favorable eligibility determination, and proximity access. The first three categories permit full access to SCI material on a need to know basis, provided a full background investigation is completed. The fourth category grants procedural access to SCI rather than substantive access and is generally used for a person who is located near the processing of SCI material but does not have a need for substantive access. For example, proximity access would be granted to a receptionist in a SCIF who may pass the SCI material coming from a courier to a bona fide reader/processor of SCI.

(U) Next, DS/SSO notifies PSS, IND, and the requesting bureau of the decision to grant SCI access. DS/PSS enters the information into the appropriate database, CMS or [redacted] respectively. DS/SSO notifies the individual via e-mail, memorandum, or telegram and schedules the indoctrination briefing. DS/SSO notifies individuals at overseas posts, through telegrams to the regional security officer (RSO), and the post's SCI Control Officer provides the indoctrination briefing. The individual is responsible for following up and confirming the briefing. After the individual attends the indoctrination briefing, he or she must sign an NdA, which DS/SSO maintains.

Denial of SCI Access (U)

(U) When the DA denies SCI access, he first informs the SOIC of his intentions and obtains his concurrence. The DA then informs the individual by memorandum of the reasons for denial and of his/her appeal rights. He also informs the requesting bureau of his determination, but in consideration of privacy issues, does not include the reason(s) for denial. Where appropriate for assignment purposes, HR is also informed of the denial. DS/SSO provides copies of all memoranda to DS/PSS, which becomes the repository for memoranda relating to the decision. An individual may appeal his/her denial by requesting that the DA review the case or the individual may file a formal appeal requesting that the SOIC convene an appeals panel. Appeals may be submitted in writing or the individual may appear in person.

Effect of DS Adverse Action Process on SCI Access (U)

(U) The DS Adverse Action branch, located within the Office of Security Infrastructure, Personnel Security Suitability division, adjudicates cases of employee misconduct concerning criminal activity, or alcohol and drug abuse and determines whether to suspend, revoke or take other action against an individual's security clearance. If DS suspends or revokes the security clearance, the DA must revoke the individual's SCI access. If DS elects not to suspend or revoke the security clearance, it issues a warning or puts employee's clearance on probation. After DS adjudicates the case, it sends a letter to the DA stating the results of the adjudication. The DA has discretion to revoke or permit the employee's SCI access if the employee receives a warning or his/her security clearance is put on

probation. The employee may appeal the process and if the employee is successful and wins reinstatement of his/her security clearance, the DA will normally reinstate the SCI access. DS/SSO records security clearance suspension and probation information into [redacted]

Revocation of SCI Access (U)

(U) If an individual no longer needs SCI access because he or she has retired, terminated his or her employment with the Department, transferred to another bureau, or have died, the employee's bureau should notify DS/SSO so that the individual's name can be removed from SCI access databases. The DA has discretion to administratively remove employees from SCI access if they have transferred to another bureau within the Department where access is not required. To address the majority of personnel actions affecting SCI access, HR provides a monthly update to DS/SSO listing all employees who have retired, transferred within the Department, terminated their employment, or passed away. DS/SSO matches this listing against its database of individuals with active SCI access and determines whether or not the SCI access is still required. DS/SSO must receive formal notice either via telephone, e-mail, or memorandum that an employee within the Department who has transferred to another office or bureau no longer needs the access.

Temporary SCI Access (U)

(U) DS grants temporary SCI access to individuals who have not received completed background investigations, but due to national emergency situations require access. For example, individuals needed in a war zone would receive such access. The temporary access is granted for a specific period of time until their permanent security clearance is issued. The DA has the option to either grant or deny SCI access to personnel who have temporary security clearances based on a review of their file and pertinent background information.

OIG Assessment (U)

(U) The Department's management of the process to grant SCI access meets DCID requirements. Through observation, examination, and detailed testing, OIG found that DS properly conducted background investigations and reviewed available background security files to determine each individual's eligibility for SCI access. However, OIG found that [redacted]

(U) To review the process of granting SCI access, OIG requested a sample of 60 files, involving those Department employees, contractors, and WAE employees who were granted or denied SCI access from March 1, 2003 to February 29, 2004. OIG reviewed the background investigation files to determine if the SSBI process was performed in accordance with DCID 6/4 and Department policy. OIG found that DS/PSS thoroughly and properly reviewed each individual's background files and properly determined whether any immediate family members who were born as foreign nationals presented national security concerns. However, OIG [redacted]

(U) To test the process for maintaining files and performing SSBI checks for SCI access, OIG reviewed the 57 available files to ensure that the investigative requirements in DCID 6/4, Standard B, were addressed. OIG observed that the files contained information such as the documented need for SCI access, a completed SSBI, waivers for SCI access, memoranda describing a compelling need, the indoctrination briefing date, the signed NdA, completion of local agency checks and national agency checks, and a review of foreign connections. OIG also found that almost all of the necessary items were present in each of the 57 files in hard-copy form or had been entered into the CMS database. [redacted]

(U) DCID policy requires that the investigative requirements be verified, but it does not dictate how the supporting details should be maintained. Because the Department should ensure that all items have been verified, OIG believes that DS [redacted]

(U) Although OIG believes that these issues should be addressed, it does not believe the issues have material implications in the management of the SCI access process.

(U) **Informal Recommendation 1:** [redacted]

(U) **Informal Recommendation 2:** [redacted]

(U) DS concurs with these recommendations.

SCI SECURITY AWARENESS AND TRAINING PROCEDURES (U)

(U) The Department meets DCID requirements for training personnel who have SCI access and for the Special Security Representatives (SSRs) who provide advice and assistance to SCIF members. The Department ensures that individuals are indoctrinated prior to using their SCI access, provides periodic security awareness training, and debriefs individuals when they no longer need SCI access. The Department also provides indoctrination training and periodic security awareness training to its SSRs.

Requirements (U)

DCID Requirements (U)

(U) DCID 6/4 requires member departments and agencies to establish continuing security programs, based on risk management principles, for all individuals that have access to SCI material. The agencies must indoctrinate the individuals, monitor their performance and security postures, and resolve issues that question an individual's loyalty and integrity. The agencies must implement security education programs that will enhance the security awareness of the U.S. civilian and military personnel and private contractors with SCI access and ensure that SCI material is safeguarded. These programs must be documented, to ensure that all personnel receive the training. The DCID splits security awareness requirements into three categories: initial indoctrination, continuing security awareness programs, and guidelines and instructions for terminating SCI access.

(U) As a condition for gaining access to SCI, individuals must sign a DCI-authorized SCI NdA, which includes a provision for prepublication review. Failure to sign an NdA is cause for denial or revocation of SCI access. The NdA establishes explicit obligations for both the government and the individual signing it.

(U) Prior to signing the NdA or being afforded access to SCI, persons approved for SCI access are to be given a non-SCI-revealing briefing on the general nature and procedures for protecting SCI and advised of their obligations to protect that information and to report matters of security concern. They are also allowed to express any reservations concerning the NdA or access to SCI. (Persons unwilling to sign the NdA or to accept SCI security obligations are not to be granted SCI access.) This indoctrination must include information on such matters as the need for and purpose of SCI, the intelligence mission of the requesting department or agency, the definitions and criminal penalties for espionage, administrative sanctions for violating security procedures, and a description of security responsibilities and obligations for reporting foreign travel and other activities and conduct of personnel.

(U) Additionally, each agency must establish a continuing security awareness program to ensure that personnel obtain frequent exposure to security-awareness material. The programs must include elements such as the foreign intelligence threat, technical intelligence threat, the administrative, personnel, physical and procedural

threats; and special security briefings and debriefings. The programs can be presented as live briefings, pamphlets, fliers, or audiovisual presentations. The agencies must use current information and materials, and the programs should meet the needs of the department or agency.

(U) Appropriately SCI-indoctrinated special security officers and/or SCI control officers and their alternates, are to be designated to operate each SCI Special Security Office and/or Control Center. Such officials shall normally have day-to-day SCI security cognizance over their offices or centers and subordinate SCIFs regarding the SCI material handled by the organizations they serve. Responsible SOICs must train their SCI special security/control officers and other SCI registry/security personnel regarding SCI security policies and procedures. SCI Special Security/Control Officers, in turn, must provide advice and assistance on SCI matters to their organizations and the activities they support, consistent with specific responsibilities assigned by their SOICs. This may include:

- Ensuring that SCI is properly controlled, transmitted, destroyed, packaged, safeguarded, and where appropriate, brought under accountability.
- Giving advice and guidance on SCI classification matters, sanitization, downgrading, decompartmentization, and operational use.
- Ensuring that SCI is disseminated only to persons authorized access to the material involved and having an established need-to-know.
- Conducting or managing required SCI personnel and physical security actions and procedures.
- Investigating SCI security infractions and preparing reports and recommendations as required.
- Interfacing, as required, with SCI telecommunications centers, the facilities of Automated Information Systems (AIS), and with similar offices to ensure SCI security. Interaction between SCI Special Security/Control Officers and Information Systems Security Officers (ISSOs), appointed pursuant to DCID 6/3, is particularly important in ensuring the security of both SCIFs and the AIS network components housed in SCIFs.

(U) Finally, when an agency has determined that access to SCI is no longer required, individuals must receive final instructions and guidelines. The agencies involved must ensure that these individuals are cognizant of pertinent sections of the laws describing criminal sanctions for espionage and of their continuing obligation to safeguard any SCI material that they may recall. The individuals must also declare that they do not have SCI material when they relinquish their SCI access and must be reminded of the risks associated with foreign travel and foreign association.

SCI Awareness Training Procedures (U)

SCI Indoctrination Procedures (U)

(U) Each person, after being granted SCI access but before being afforded access to SCI must receive an indoctrination briefing from DS/SSO on the procedures for protecting SCI and sign an NdA. Upon signing the NdA and receiving the indoctrination, the person's name is recorded in the DS/SSO SCI database [redacted], which are used to identify SCI-cleared individuals.

Periodic Security Awareness Training (U)

(U) The Department's SCI-awareness training consists of three types of training or briefings, as required by DCID 6/4. The types of training, each identified in italics below, are:

Periodic Awareness Enhancement (U)

(U) DS/SSO provides training through special SCI security training classes, its Web site, and periodic SCI briefings that each SSR provides to each SCIF member to meet the DCID's continuing SCI security awareness requirements. The Department is developing an electronic, periodic, SCI-awareness training program and circulating a Department Notice entitled, "Responsibilities of Personnel with SCI Access."

(U) Special training sessions: DS/SSO provides special SCI security-awareness training classes to bureau employees upon a bureau's request. At this time, DS/SSO had provided this special training session to four bureaus in calendar year 2004.

(U) DS Web site: During the initial SCI indoctrination briefing, participants are informed about the DS Web site and how to access it. The site contains information for SCI-cleared personnel, reiterating their SCI security responsibilities.

(U) SSR Briefings: A primary and, generally, a secondary SSR are appointed for each of the Department's SCIFs by the bureau in which the SCIF is located. SSRs are responsible for liaison with DS/SSO, the day-to-day operational security requirements within the SCIF, and periodic SCI security awareness training for all SCIF members.

(U) DS/SSO is developing for SCI-indoctrinated personnel a periodic, electronic, SCI-awareness training program similar to the annual DS security briefing provided to Department employees via a compact disk. This effort is in the planning stage, and DS plans to track this training to ascertain that each SCI-indoctrinated individual has received annual SCI awareness training.

(U) A Department Notice, 2004-09-099, dated September 2004, and titled "Responsibilities of Personnel with SCI Access," was circulated to all Department personnel reiterating the responsibilities of personnel with SCI access.

SSR Training (U)

(U) SSRs are appointed to each of the Department's SCIFs by the bureau in which the SCIF is located. SSRs are responsible for liaison with DS/SSO, the day-to-day operational security requirements within the SCIF, and providing periodic SCI security awareness training to all SCIF members. When SSRs are appointed, DS/SSO provides them with SSR training. Annually, SSRs are provided with refresher training during DS/SSO annual Periodical Security Reviews (PSRs) of the Department's SCIFs. DS/SSO also provides special training classes to bureaus that request additional SSR training. The SSR's training is recorded on DS/SSO's SCI database. As of December 2004, DS/SSO has conducted PSRs in [redacted] of the Department's [redacted] SCIFs.

Debriefings (U)

(U) Generally, individuals that receive SCI access maintain it throughout their careers. However, when SCI-indoctrinated individuals leave the Department, DS/SSO records on the SCI access database that these individuals are no longer employed and are no longer indoctrinated for SCI. In this "administrative debriefing," the Department advises employees of the debriefing requirement through guidance published in the FAM and through the NdAs that employees sign when they receive SCI access. In 12 FAM 564.4, personnel are advised of their responsibility to receive a debriefing when they terminate employment or are otherwise separated from employment for a period of 60 days or more. Individuals and contractors that no longer require SCI access or leave the Department are to contact DS/SSO to receive an SCI debriefing in person.

(U) In the SCI indoctrination briefing, the refresher briefing, and the information provided when the NdA is signed, the individual is informed of the following specific debriefing requirements. The requirements involve:

- the continuing obligation, under the prepublication and other provisions of the SCI NdA, never to divulge SCI to any unauthorized persons without the written consent of appropriate department/agency officials; and
- the requirement that the individual may no longer possess any documents or material containing SCI.

OIG Assessment (U)

SCI Indoctrination Procedures (U)

(U) The Department's SCI-indoctrination procedures meet DCID requirements. OIG reviewed the process, identified the controls that restrict SCI access

for individuals prior to indoctrination, attended an SCI indoctrination briefing, ascertained that the SCI indoctrination briefing meets DCID 6/4 topic requirements, and confirmed that signed NdAs are on file for 57 of the 60 Department personnel in our sample who had SCI access. The remaining 3 personnel did not have signed NdAs because they were denied SCI access.

Periodic Awareness Enhancement (U)

(U) The Department's SCI periodic awareness enhancement program meets DCID requirements. OIG confirmed that, during the SCI indoctrination briefings, participants learned how to access SCI security awareness information, including using an on-line, periodic SCI-training program from DS's Web site. OIG reviewed the Web site and the periodic training program and found them detailed and comprehensive. OIG attended an annual SCIF periodic security review and ascertained that the SCIF's SSR had received an SCI refresher briefing and had been informed of his responsibility for providing SCIF members with periodic security-awareness training. The SSR also provided training dates for his SCIF members. DS/SSO security personnel informed OIG that personnel from four Department bureaus received additional special SCI training. Annually, DS/SSO provides all SSRs with SCI training. OIG reviewed the draft Department Notice entitled "Responsibilities of Personnel with SCI Access" and determined that the Notice was detailed and comprehensive and adequately described SCI responsibilities. The Department issued the Notice in September 2004.

(U) Additionally, OIG sampled a group of individuals assigned to Department headquarters who received SCI access during the period January 2000 through December 2003. OIG interviewed these individuals to determine if they had received additional SCI security awareness training since their indoctrination briefing and to assess the effectiveness of the training. OIG asked the 10 individuals interviewed questions to ascertain their awareness of their SCI responsibilities. OIG found that all felt confident about their SCI responsibilities, knew how to obtain security assistance, if necessary, and had been exposed to SCI security awareness briefings or training after receiving their initial indoctrination briefing. OIG believes the Department is properly providing SCI security awareness training for personnel.

Debriefings (U)

(U) The Department's SCI debriefing process meets DCID requirements. OIG was informed that the Department debriefs individuals using one of two DCI-accepted methods and that the debriefings occur in person or are done administratively. OIG was informed that between April 1 and July 4, 2004, in 72 percent of the debriefings, DS/SSO met with the individuals in person, properly debriefed them, and ensured that the debriefing-acknowledgement portion of the NdA was signed. DS administratively debriefed the remaining 28 percent .

(U) OIG consulted with the DCI's staff to ensure that the process to debrief individuals included administrative debriefing and confirmed that the DCI permits in-

person and administrative debriefing and that these methods are widely used in the intelligence community. DS informed OIG that sometimes individuals with SCI access do not receive a personal debriefing when they no longer require SCI access, because these persons did not initiate the debriefing process with DS/SSO. Although personnel are advised of the debriefing requirement by guidance in the FAM and the NdA, they do not always contact DS to receive the debriefing. DS/SSO often becomes aware that the individual no longer needs SCI access when it examines the monthly electronic download that HR provides to the DS/SSO SCI access database and notices changes in personnel. DS compares its SCI roster with HR's list, to ensure that the SCI roster contains current Department employees, and it uses the information to administratively debrief the employees who have not been personally debriefed and removes their name from the SCI access roster. DS/SSO notifies appropriate DS offices, such as the Building Pass Unit, to ensure that the individuals no longer have access to Department facilities. OIG made no recommendations in this area, as the process met DCID requirements.

SECURITY POLICY CONCERNING TRAVEL AND ASSIGNMENT OF PERSONNEL WITH SCI ACCESS (U)

(U) The Department's policies and procedures provide an effective means for its personnel with SCI access to meet DCID requirements concerning travel or assignment to hazardous countries. Such policies and procedures advise SCI-indoctrinated individuals regarding the requirement to report official and unofficial foreign travel and on how to obtain necessary defensive-security briefings. Although they are effective, the procedures could be improved by [redacted] Additionally, the Department should monitor the status of DCID 6/10, which is in draft and will replace DCID 1/20(P), and amend Department policies or procedures as needed when the new DCID is issued.

Requirements (U)

DCID Requirements (U)

(U) DCID 1/20(P) requires SCI-indoctrinated personnel traveling on official and unofficial travel to security-risk countries designated by the DCI to report their itinerary in advance and receive a defensive-security briefing. Additionally, the SSO must maintain a travel file for SCI-indoctrinated personnel. Hazardous travel includes travel to countries or missions listed in the Annex to the DCID, or traveling via the national transportation carriers of those nations, or traveling to combat zones and other areas where the physical safety and security of personnel and SCI cannot be reasonably assured. Persons are discouraged from personal travel to the countries listed in the Annex. Failure to comply with provisions for reporting travel would result in the withdrawal of approval for continued access to SCI and could affect the granting of future SCI access.

(U) The DCI is responsible for ensuring that a list of countries identified as posing a security risk is updated and disseminated to the SOICs. The SOIC must review proposed

unofficial hazardous travel and decide whether to retain or withdraw SCI access for travelers. In advance of travel for official or unofficial purposes, travelers must submit an itinerary to an official specified by the cognizant SOIC, receive a defense-security and/or risk-of-capture briefing from an official specified by their cognizant SOIC. The traveler must also immediately contact the nearest U.S. diplomatic facility if he or she is detained or subjected to harassment and provocation while traveling, and on returning from travel, report any unusual incidents to the cognizant security official.

(U) In 1994, the DCI discontinued using the DCID Annex's list of security-risk countries and is developing a new list that will be included in DCID 6/10. The DCI's Special Security Center (DSSC), however, provided OIG a current official interpretation for DCID 1/20(P), asserting that the DCID continues to provide valid requirements although the directive does not include the Annex. The DCID primarily requires personnel with SCI access to report travel to specific countries that are defined as "hazardous." Also, the DCID defines minimally acceptable practices, and the SOIC may implement a more stringent policy that requires reporting all foreign travel. According to DSSC, the standard practice in the intelligence community is that those who have access to SCI report all foreign travel to the cognizant SOIC.

Other Requirements (U)

(U) DS/SSO issued a Department Notice entitled "Responsibilities of Personnel with SCI Access" and dated September 28, 2004. The Notice reminds individuals with SCI access of their special reporting responsibilities. Specifically, those individuals must report activities or conduct concerning themselves or others that might affect their ability to protect classified information from unauthorized disclosure. Additionally, they must report unofficial travel to any foreign country and report official and unofficial travel to any nation that has received a ***critical*** threat rating for its human intelligence threat. DCID 1/20P contains detailed items that require reporting, and the Notice is the SOIC's policy to implement the DCID within the Department.

(U) According to 12 FAM 264, entitled "Personal Travel to Critical Human Intelligence Threat Countries," all U.S. government employees under the authority of a chief of mission must notify the RSO or Post Security Officer (PSO) in advance of intended personal travel to any country with a ***critical*** human intelligence threat. Employees stationed domestically should notify the DS/ICI/CI three weeks prior to travel. Each employee should provide the information using a specific form and the RSO, PSO, or DS should keep the information on file. Additionally, the RSO, PSO, or DS must give each traveler a defensive-security briefing prior to the travel. The Department maintains a list of ***critical***-threat countries; it was developed through the Overseas Security Policy Board.

Security Policy Procedures for SCI-Indoctrinated Personnel (U)

(U) The DCID policy information on travel to hazardous countries is provided by the Department during the SCI-indoctrination briefing and in Department Notices. The

Department also plans to have employees formally accept responsibility for reporting such information during future indoctrination briefings. The requirement to have personnel report travel or receive defensive security briefings changed in 1994 when the DCI discontinued using the DCID 1/20(P)'s list of hazardous countries. The DCI is revising DCID 1/20(P) and DCID 6/10 will supercede it when that DCID is issued.

(U) The Department notifies personnel to report foreign travel by issuing guidance in the FAM and in periodic Department Notices. Typically, personnel with SCI access who take personal trips to foreign countries contact DS/SSO, which determines whether the person is traveling to a nation rated as posing a ***critical*** human intelligence threat. If the travel does not, the traveler is referred to the DS Website, to review the "Personal Travel Notifications 12 FAM 264" briefing. If the travel does involve a ***critical*** human intelligence threat country, the traveler is referred to the counterintelligence office in DS/ICI/CI and receives a defensive-security briefing. However, DS/SSO does not have complete records of these contacts because some personnel may be contacting DS/ICI/CI directly or may be failing to report personal travel. DS/SSO plans to incorporate a section on its Website that addresses reporting temporary-duty travel requirements for SCI-indoctrinated personnel.

OIG Assessment (U)

Reporting Foreign Travel (U)

(U) OIG found that DCID 1/20(P) requirements for reporting foreign travel to the SOIC did not specifically require SCI-indoctrinated personnel to report all unofficial and official foreign travel. Instead, the DCID only required the reporting of travel to those countries defined as "hazardous" and identified in its annex. However, OIG found that, [redacted] To address this, the Department issued a Department Notice on September 28, 2004, advising that SCI-indoctrinated personnel must report to the applicable SCI Facility SSRs or DS/SSO any unofficial foreign travel and official and unofficial travel to a nation having a ***critical*** threat rating for human intelligence. OIG consulted with the DSSC and found that it plans to replace DCID 1/20(P) with DCID 6/10 soon. [redacted]

(U) OIG obtained the official interpretation for DCID 1/20(P) from the DSSC, which stated that it primarily requires personnel with SCI access only to report travel to specific countries defined as "hazardous." But, because the DCID defines only the minimally acceptable practices, the SOIC may implement a more-stringent policy that requires the reporting of all foreign travel; this is standard practice in the intelligence community. Therefore, because the Department Notice is the SOIC's official interpretation of the DCID, OIG agrees with its travel reporting requirements. The Department should

monitor the status of DCID 6/10 and change Department policy as necessary to implement the new DCID's requirements, when it is issued.

Recommendation 1: (U) The Bureau of Diplomatic Security's Special Security Office should monitor the status of draft DCID 6/10 and advise the Department's Senior Official of the Intelligence Community when DCID 6/10 becomes official. (Action: DS)

(U) DS concurs with this recommendation.

Reporting Inconsistencies Within the Department (U)

(U) OIG found that [redacted]

Recommendation 2: (U) The Department should [redacted] (Action: DS)

(U) DS concurs with this recommendation.

B. AUTOMATED INFORMATION SYSTEMS SECURITY (U)

PROTECTION OF SCI INFORMATION WITHIN INFORMATION SYSTEMS (U)

~~(SBU)~~ The Department's policies and procedures, taken as a whole, comply with the requirements for protecting SCI material within automated information systems described in DCID 6/3. The division of roles and responsibilities between INR and DS meets the directive's requirements, [redacted]

[redacted]

SCI INFORMATION SYSTEMS (U)

(U) [redacted] All SCI systems within the Department are under the purview of the principal accrediting authority – the Assistant Secretary for INR. [redacted] received authorities to operate in 2004.

Requirements (U)

DCID Requirements (U)

(U) DCID 6/3 specifies the requirements for protecting SCI material stored or processed on automated information systems (AIS). This directive requires the Department to have an information system security program that complies with technical and administrative security requirements and is supported by appropriate documentation.

(U) [redacted]

(U) [redacted]

(U) The DAA is responsible for ensuring that documentation is maintained for all information system accreditations within its purview. The DAA representative is responsible for developing and overseeing the implementation of the security policy and for providing guidance for securing SCI AISs.

Other Requirements (U)

(U) DS developed the Department of State Sensitive Compartmented Information Systems Security Standards (DSSCISSS) to provide procedural guidance relative to the management of SCI and the automated infrastructure. The supplemental guidance

addressed day-to-day information system security issues at the organizational level and was revised in July 2003. Concurrently, DS created an SCI Systems Concept of Operations and Standard Operating Procedures manual, to provide procedures and requirements for managing and operating SCI networked information systems. The guidance also applies to unclassified and collateral AISs within INR or other SCIFs within the Department.

ROLES AND RESPONSIBILITIES (U)

(U) The division of the roles and responsibilities between INR and DS meets the requirements of DCID 6/3. On May 24, 2000, the Assistant Secretary of INR transferred to DS specific security responsibilities for the protection of SCI. These responsibilities, outlined in a memorandum of agreement dated March 2001, required DS to develop directives for the implementation of all relevant DCIDs and oversee agency compliance with those DCIDs and implementing directives (DSSCISSS and SCI Systems Concept of Operations and Standard Operating Procedures). Under the agreement, DS is the designated accreditation authority, the Assistant Secretary of INR is the PAA and the data owner of [redacted] and the ISSM and ISSO are employees of INR. Specific roles and responsibilities are described in the DSSCISSS.

DCID Requirements (U)

(U) The PAA exercises top-level management oversight, ensuring that all processes and procedures are established, implemented, and maintained. In general, the PAA's operational authority is delegated to the DAA. The DAA assumes formal responsibility for operating the system at an acceptable risk level, based on the implementation of an approved set of technical, managerial, and procedural safeguards. The DAA representative ensures that security is integrated into and implemented throughout the life cycle of the system. The ISSM is responsible for the organization's information system security program, and the ISSO is responsible for ensuring operational security is maintained for a specific network. Privileged Users have access to the system's control, monitoring, and administration functions.

Department Procedures (U)

(U) The Assistant Secretary for INR is the PAA for [redacted] and is the data owner of [redacted] The Director of Intelligence and Threat Analysis in DS is the data owner of [redacted] The PAA has delegated the operational authority for the Department's SCI systems to DS/SI/IS.

CONFIDENTIALITY AND INTEGRITY (U)

~~(SBU)~~ The Department has established the levels of concern and protection level for its SCI systems, as required by the DCID. This combination of security controls, implemented by personnel and the system, addresses the confidentiality and integrity protection requirements. However, improvements are needed [redacted]

[redacted]

Requirements (U)

DCID Requirements (U)

(U) Federal agencies must ensure that (1) individuals are held accountable for their actions, (2) information is accessed by authorized personnel, (3) information is used only for authorized purpose(s), (4) information retains its content integrity, (5) information is available to satisfy mission requirements, and (6) information is appropriately marked and labeled. To provide confidentiality, each AIS controls the release of information commensurate with the sensitivity of the information being processed. To protect the integrity of information, each AIS ensures that its resistance to unauthorized modifications is commensurate with its determined integrity level of concern.

(U) SCI systems must be assigned a protection level and a levels-of-concern rating for integrity and availability. This designation must be in writing and operational for the life of the system. For example, [redacted]

(U) A formal incident reporting program must be in place and evaluated regularly by the DAA. Procedures are developed by the ISSM and approved by the DAA. All security incidents are required to be reported to the DAA and the data owner.

Other Requirements (U)

(U) The DSSCISS requires all privileged users to maintain a separate General User account that is to be used at all times except, when the Privileged User performs System Administration functions. The SCI Systems Concept of Operations and Standard Operating Procedures requires accounts that have been inactive for more than 90 days to be reviewed for deletion.

Department Procedures (U)

~~(C)~~ The DAA has designated all SCI systems in the Department as [redacted]

(U) SCI systems in the Department are controlled through physical, administrative, or technical means or by a combination of these. For example, physical controls require personnel to sign a roster to enter the SCIF, preventing visitors from wandering around. Administrative controls include procedures for obtaining supervisory approval to receive

system access as well as two information security briefings, the general-user briefing and another ISSO briefing. Technical controls include the auditing of all files and data for failures and the use of National Security Agency-approved software to encrypt transmitted data.

(U) The combination of controls provides the required confidentiality and integrity for the information. Users who need to download or upload information from a diskette must request a floppy drive from the ISSO. Users who receive the drive, sign receipts and are fully responsible for it. [redacted] Users are notified before accessing the system that their activities may be monitored, recorded, and subject to audit. If a computer is idle for more than 15 minutes, the system automatically locks the user out, and the user is required to re-enter his password to obtain access again. Previously entered information is not visible on monitors when workstations are locked. Users must change passwords every 180 days.

(U) A security incident is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security policies. When a security incident is identified, the ISSO investigates and, each week, informs the point of contact for the Intelligence Community-Incident Response Center (IC-IRC). The information includes all security incidents and describes the incident, when it occurred, what steps were taken to eliminate the incident, and how many workstations and servers were affected. The ISSO only reports physical security compromises to DS. This limited reporting does not comply with the requirement that the DAA be informed of all security incidents.

~~(SBU)~~ OIG found [redacted]

~~(SBU)~~ [redacted]

AVAILABILITY (U)

~~(SBU)~~ [redacted]

Requirements (U)

DCID Requirements (U)

(U) Each AIS must implement security features that ensure information is available for use when, where, and in the form required for its availability level-of-concern rating. There must be frequent back-ups, and back-up storage must be available on- and off-site. The ISSO or ISSM should test the AIS periodically by using various intrusion- and attack-detection and monitoring tools. All AISs must have a contingency/disaster recovery plans, and the DAA representative must verify that the necessary security procedures and mechanisms are in place and test them.

Department Procedures (U)

~~(SBU)~~ [redacted]

~~(SBU)~~ [redacted]

~~(SBU)~~ Although DS updated the contingency plan when developing the SSP in July 2004, [redacted]

SECURITY AWARENESS TRAINING AND EDUCATION (U)

~~(SBU)~~ [redacted]

Requirements (U)

DCID Requirements (U)

(U) The DAA assures that a systems-security, education, training and awareness program is developed and implemented. All administrators and users must complete security education, training, and awareness.

Department Practices (U)

(U) When they receive their initial SCI access, DS/SSO trains its personnel on handling, accounting for, and storing SCI material. Also, DS/SI/IS has training programs for General Users and Privileged Users, and the former is computer-based training. The Privileged User training is for the system administrators, system managers, ISSMs, and ISSOs. No Privileged User training has been given to date, because there is no trainer.

(U) The ISSO takes many steps that are above what the DCID requires. Before creating an SCI computer account, the ISSO provides each user with a security briefing. This briefing is in addition to the initial security briefing given by DS when the individual obtains SCI access. Also, to increase security awareness, the ISSO has created labels that are placed on each machine to remind users that the Department may monitor the system at any time.

CERTIFICATION AND ACCREDITATION (U)

(C) The Department's procedures for certifying and accrediting SCI systems are in compliance with DCID 6/3. All of the Department's SCI systems are certified as [redacted] received their accreditations in August and November 2004, respectively.

Requirements (U)

DCID Requirements (U)

(U) The certification process validates the appropriate levels-of-concern and protection levels. The accreditation of an AIS is the official management decision to operate an AIS in a specified environment. The DAA can grant interim approval to operate (IATO) or approval to operate. IATOs may be granted for up to 180 days and can be renewed once for an additional 180 days. After 360 days, the system must be

accredited or terminated. The DCID requires all certified and accredited systems to be implemented in five phases, the last of which is disposal of the system.

(U) The DAA is responsible for ensuring documentation is maintained for all information system accreditations within the DAA's purview.

Department Practices (U)

(U) The PAA has delegated the accreditation and certification of SCI systems to the DAA. The DAA maintains all accreditation paperwork. DS accredited the [redacted] systems using the established guidelines in DCID 6/3.

~~(SBU)~~ In 2001, DS/SI/IS received authority to accredit SCI systems for the Department. INR reduced the number of vulnerabilities from 26,387 to 90 during 2003 [redacted] received separate authorities to operate on August 1 and November 24, 2004, respectively.

OIG Assessment (U)

~~(SBU)~~ The Department's policies and procedures, taken as a whole, comply with the requirements for protecting SCI material within AISs, as described in DCID 6/3, but [redacted]

~~(SBU)~~ [redacted]

(SBU) [redacted]

~~(SBU)~~ There are [redacted] Privileged Users on the [redacted] system. DCID 6/3 states that the system should be limited to the minimum number of Privileged Users needed to manage the system. In addition, the DSSCISSS states that all Privileged Users should have a General User account in addition to their administrative account.

~~(SBU)~~ INR's checklist shows that departing bureau personnel are to check out with the system manager. However, [redacted]

~~(SBU)~~ [redacted]

(U) [redacted]

(U) To address these deficiencies, OIG recommends the following:

Recommendation 3: (U) [redacted] (Action: INR)

(U) INR concurs with this recommendation. The current situation is a temporary one created when the [redacted] System Manager retired last year. The deputy system manager, who is also the ISSO, has been promoted recently to the system manager position. The deputy system manager position is in the process of being advertised.

Recommendation 4: (U) [redacted] (Action: INR)

(U) INR concurs with this recommendation.

~~(SBU)~~ [redacted]

Recommendation 5: (U) [redacted] (Action: INR)

(U) INR concurs with this recommendation.

(U) [redacted]

Recommendation 6: (U) [redacted]. (Action: INR)

(U) INR concurs with this recommendation.

(U) [redacted]

Recommendation 7: (U) [redacted]. (Action: INR)

(U) INR concurs with this recommendation.

(U) [redacted]

Recommendation 8: (U) [redacted] (Action: INR)

(U) INR concurs with this recommendation.

(U) [redacted]

Recommendation 9: (U) [redacted]. (Action: INR)

(U) INR concurs with this recommendation.

~~(SBU)~~ [redacted]

Recommendation 10: (U) [redacted] (Action: DS)

(U) DS concurs with this recommendation.

Recommendation 11: (U) [redacted] (Action: INR)

(U) INR concurs with this recommendation.

(U) [redacted]

Recommendation 12: (U) [redacted]
(Action: DS)

(U) DS concurs with this recommendation.

C. DOCUMENT CONTROL FOLLOW-UP (U)

(U) OIG determined during its 2003 calendar year review that the Department's procedures for handling and controlling accountable SCI documents, from initial receipt to final storage or destruction, provided an effective method to meet DCID requirements and other applicable control procedures. However, OIG found [redacted] The Department concurred with the recommendations and has taken steps to implement them. The following three issues arose during the 2003 year review, and the Department's progress in implementing the recommendations is included below.

SEIB Reader Lists and Pouch Pick-Up Lists (U)

(U) OIG observed during the 2003 review that the process to control accountable SCI material met DCID requirements, but [redacted]

[redacted]
more difficult to track documents that are lost or compromised during transmission.

(U) OIG recommended [redacted]

(U) OIG met with DS officials and reviewed the procedures for implementing the recommendation. [redacted]

SCI Pouch Control Procedures for Non-Accountable Documents (U)

(U) During the 2003 audit, OIG concluded that the Department's procedures for handling non-accountable SCI documents complied with DCID requirements, but that the Department needed to [redacted]

(U) During the 2003 audit, OIG met with the DCI staff to obtain an official interpretation of the DCID requirements for tracking non-accountable documents and discovered that [redacted]

[redacted]

~~(SBU)~~ DS concurred with the recommendation and stated that it [redacted]

~~(SBU)~~ OIG reviewed a sample [redacted]. OIG concluded that DS and INR have taken sufficient steps to meet the intent of Recommendation 2 from the 2004 report and that recommendation is closed.

SCI Handling Guidance (U)

(U) During the 2003 audit, OIG observed that [redacted]

~~(SBU)~~ DS and INR officials generally concurred with the recommendation and formally responded that the following steps were taken and were consistent with DCID requirements:

[redacted]

[5] Because Department Notices expire after one year, OIG recommended that the Department issue frequent reminder notices.

[redacted]

~~(SBU)~~ OIG met with DS officials to discuss the implementation of this recommendation, and DS said [redacted]

~~(SBU)~~ OIG also reviewed the information on the Department's Website [redacted]

~~(SBU)~~ OIG looks forward to the publication of the SCI document-handling guidance in the FAM and finds the steps DS has taken and plans to take sufficiently meet the intent of Recommendation 3. Recommendation 3 from Report No. SIO/A-04-11 is closed.

D. SCI PHYSICAL SECURITY (U)

(U) OIG determined during the 2003 review that the Department's SCIF-accreditation and certification process provides a comprehensive and effective method for the Department to meet DCID requirements. OIG found that the Department established an effective program to ensure that accredited SCIFs and SCIF procedural security continually met DCID requirements. During the 2004 review, OIG verified that the Department maintained the same process to accredit and certify the SCIFs but found there will soon be a minor change in responsibility for reporting to Congress. The DCI's Special Security Center will assume responsibility for certifying the SCIFs to Congress, [redacted] The only area that OIG questioned during the 2003 review that merited follow-up review was the management of the number of SCIFs that the SSRs oversee.

(U) In its 2003 review, OIG reported that it planned to follow-up on the issue addressing limiting the number of SCIFs that SSRs oversee. OIG recommended [redacted]

[redacted] After reviewing the response and discussing the issue with DS, OIG deleted the recommendation from its final report.

(U) During the 2004 review, OIG revisited this issue and obtained an updated listing of the SSRs and their corresponding lists of SCIFs, SWAs, and TSWAs. [redacted] Therefore, OIG concluded that DS is adequately managing the process to provide day-to-day oversight for facilities handling, controlling, and processing SCI material.

E. [redacted] (U)

(U) [redacted]

(U) The Department agreed. [redacted] Recommendation 4 from SIO/A-04-11 remains resolved and is reissued as Recommendation 13.

Recommendation 13: [redacted]. (Action: HR, in coordination with DS)

(U) HR concurs with this recommendation [redacted].

(U) DS concurs with this recommendation.

RECOMMENDATIONS (U)

Informal Recommendation 1: (U) [redacted] (Action: DS)

Informal Recommendation 2: (U) [redacted] (Action: DS)

Recommendation 1: (U) [redacted] (Action: DS)

Recommendation 2: (U) [redacted] (Action: DS)

Recommendation 3: (U) [redacted] (Action: INR)

Recommendation 4: (U) [redacted] (Action: INR)

Recommendation 5: (U) [redacted] (Action: INR)

Recommendation 6: (U) [redacted] (Action: INR)

Recommendation 7: (U) [redacted] (Action: INR)

Recommendation 8: (U) [redacted]

[redacted]. (Action: INR)

Recommendation 9: (U) [redacted] (Action: INR)

Recommendation 10: (U) [redacted] (Action: DS)

Recommendation 11: (U) [redacted] (Action: INR)

Recommendation 12: (U) [redacted]. (Action: DS)

Recommendation 13: (U) [redacted]. (Action: HR, in coordination with DS)

ABBREVIATIONS (U)

AIS	Automated Information System
CIA	Central Intelligence Agency
CMS	Case Management System
DAA	Designated Accrediting AuthorityDA
DA	Determination Authority
DS	Bureau of Diplomatic Security
DS/DCB-INR	Document Control Branch-Intelligence and Research
DS/ICI/CI	Office of Investigations and Counterintelligence, Counterintelligence Division
DS/IND	Industrial Security Division
DS/PSS	Office of Personnel Security/Suitability
DS/SSO	Special Security Office
DS/SI/IS	Office of Information Security
DSL	Diplomatic security letter
DCID	Director of Central Intelligence Directive
DCI/SSC/CAPCO	Special Security Center, Controlled Access Program Coordination Office
DSSC	DCI Special Security Center
DSSCISSS	Department of State Sensitive Compartmented Information Systems Security Standards
FAM	Foreign Affairs Manual
HR	Bureau of Human Resources
IATO	Interim approval to operate
IC-IRC	Intelligence Community-Incident Response Center
INR	Bureau of Intelligence and Research
[redacted]	[redacted]
IRM	Bureau of Information Resources Management
ISSM	Information systems security manager
ISSO	Information systems security officer
NdA	Non-disclosure agreement
OIG	Office of Inspector General
PAA	Principal Accrediting Authority
SCI	Sensitive Compartmented Information
SCIF	Sensitive Compartmented Information facility
SEIB	Senior Executive Intelligence Brief
[redacted]	[redacted]
SOIC	Senior Official of the Intelligence Community
SSBI	Single-scope background investigation
SSP	System security plan
[redacted]	[redacted]
WAE	When actually employed

APPENDIX A: COMMENTS OF INR (U)

United States Department of State

Washington, D.C. 20520

January 28, 2005

INFORMATION MEMORANDUM
S/ES

~~CONFIDENTIAL~~
(~~SENSITIVE BUT UNCLASSIFIED~~ when separated from attachment)
DECL: 20300128

TO: OIG – Mr. John E. Lange, Acting

FROM: INR – Carol Rodley, Acting

SUBJECT: OIG Report – Protection of Classified Information At State Department Headquarters (SIO/A-05-13)

(U) Thank you for the opportunity to review the draft report titled "Protection of Classified Information at State Department Headquarters." INR agrees with the conclusion reached by the OIG inspection team that the Department is complying with the requirements for protecting SCI material within automated information systems (AIS) as described in DCID 6/3. INR concurs with the recommendations set forth in the report to strengthen the protection of SCI material within the AIS. Three line in/line out changes as well as specific comments pertaining to each INR action recommendation are found below.

(U) [redacted]

~~CONFIDENTIAL~~
(~~SENSITIVE BUT UNCLASSIFIED~~ when separated from attachment)
CLASSIFIED BY: Carol Rodley, INR A/S, Acting
REASON FOR CLASSIFICATION: E.O. 12958 1.4(c) and (d)
DECL ON: 20300128

(Please note that recommendations 1,2,10, 12, and 13 are not INR actions.)

(U) Recommendation 3: [redacted]

(U) INR Comment: [redacted]

(U) Recommendation 4: [redacted]

~~(SBU)~~ INR Comment: [redacted]

(U) Recommendation 5: [redacted]

(U) INR Comment: [redacted]

(U) Recommendation 6: [redacted]

(U) INR Comment: [redacted]

(U) Recommendation 7: [redacted] for deletion of their accounts before completing the out-processing procedures.

(U) INR Comment: [redacted]

(U) Recommendation 8: [redacted]

(U) INR Comment: [redacted]

(U) Recommendation 9: [redacted]

(SBU) INR Comment: [redacted]

(U) Recommendation 11: [redacted]

(U) INR Comment: [redacted]

Attachment: OIG Report: Protection of Classified Information At State Department Headquarters (SIO/A-05-13) (C)

APPENDIX B: COMMENTS OF DS (U)

United States Department of State
Washington, D.C. 20520

January 26, 2005

~~CONFIDENTIAL~~
(UNCLASSIFIED When Separated from Report)

MEMORANDUM

TO: OIG – [redacted]

FROM: DS/MGT/PPD — [redacted]

SUBJECT: Draft Review Report: Protection of Classified Information at State Department Headquarters, No. SIO-A-05-13

The Bureau of Diplomatic Security appreciates the opportunity to review the draft OIG Report No. SIO-A-05-13. Our comments and changes are attached.

Attachment:

As stated.

~~CONFIDENTIAL~~
(UNCLASSIFIED When Separated from Report)

Drafted by: DS/SI/PSS, [redacted], extension [redacted]
DS/MGT/PPD, [redacted], extension [redacted] (cover memo) [redacted]

Cleared by: DS/SI/PSS [redacted] (per [redacted])
DS/SI/IS [redacted] (per [redacted])
DS/SI: [redacted] (per [redacted])

~~CONFIDENTIAL~~
(UNCLASSIFIED When Separated from Report)