

~~SENSITIVE BUT UNCLASSIFIED~~

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

# Report of Inspection

Bureau of Diplomatic  
Security  
Directorate of Security  
Infrastructure

Report Number ISP-I-05-45, December 2004

## ~~IMPORTANT NOTICE~~

~~This report is intended solely for the official use of the Department of State or the Broadcasting Board of Governors, or any agency or organization receiving a copy directly from the Office of Inspector General. 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 the 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.~~

~~SENSITIVE BUT UNCLASSIFIED~~

# TABLE OF CONTENTS

|  |    |
|--|----|
| KEY JUDGMENTS .....                                | 1  |
| CONTEXT .....                                      | 3  |
| EXECUTIVE DIRECTION .....                          | 5  |
| POLICY AND PROGRAM IMPLEMENTATION .....            | 9  |
| Office of Personnel Security and Suitability ..... | 9  |
| Office of Computer Security .....                  | 22 |
| Office of Information Security .....               | 25 |
| MANAGEMENT CONTROLS .....                          | 39 |
| Contracting .....                                  | 39 |
| Internal Security .....                            | 43 |
| INFORMATION RESOURCE MANAGEMENT .....              | 45 |
| FORMAL RECOMMENDATIONS .....                       | 47 |
| INFORMAL RECOMMENDATIONS .....                     | 51 |
| PRINCIPAL OFFICIALS .....                          | 55 |
| ABBREVIATIONS .....                                | 57 |
| APPENDIX I - PRIOR AUDITS AND INSPECTIONS .....    | 59 |

## KEY JUDGMENTS

- The rationale underlying the creation of the Bureau of Diplomatic Security, Directorate of Security Infrastructure (DS/SI) - elevating what were formerly three divisions under separate offices and combining them under one directorate to improve overall effectiveness - has proven to be correct.
- DS/SI is customer-focused, delivering services in a timely, transparent, and practical manner. The Office of Inspector General (OIG) found that service has improved markedly since the establishment of DS/SI. The recent establishment of a customer service unit in the Office of Personnel Security and Suitability (DS/SI/PSS) will help to institutionalize DS/SI's customer service orientation.
- DS/SI's widespread use of contractors (approximately 855) is necessary and is in keeping with the President's Management Agenda goal of outsourcing. However, the practice requires cost conscious acquisition planning and close contract management.
- DS/SI/PSS has reduced the average processing time of a security clearance from 195.2 days in 2003 to 118.7 days in 2004. Fifty-two percent of clearances are completed in less than 90 days. Plans to restructure the office should result in additional improvements. DS/SI/PSS's goal is to complete 75 percent of its applicant cases within 90 days in FY 2005 and subsequent years.
- The new Report Management System (RMS) software enables background clearance information to be passed electronically to users in the investigative and adjudicative process, saving both time and personnel resources. It also gives managers the ability to monitor the processing sequence, resulting in increased employee accountability.
- Sixteen percent of a representative sample of investigative files reviewed by OIG lacked conclusive fingerprint information from the Federal Bureau of Investigation (FBI), precluding reliable cross-referencing of felony arrest records and intelligence information. DS management should institute internal controls to correct this vulnerability.



## CONTEXT

DS/SI is composed of three offices - DS/SI/PSS, Computer Security (DS/SI/CS), and DS/SI/IS. DS/SI supports the DS mission of providing a safe and secure environment for the conduct of U.S. foreign policy. DS/SI/PSS manages the Department of State's (Department) security clearance program. DS/SI/CS helps protect the Department's cyber-systems. DS/SI/IS manages the handling of classified and Sensitive But Unclassified (SBU) information, including the security incidents program.

DS/SI was established in May 2003 for the purpose of giving greater management attention to each office's programs and to facilitate the exchange of information on crosscutting issues between the directorate's three offices. It was created by combining two divisions (Information and Computer Security) from DS's Directorate of Countermeasures, and one division from DS's Office of Investigations, and elevating each to office status. The director of DS/SI is a member of the senior executive service and holds the title of senior coordinator for security infrastructure.

The last inspection of DS as a whole was conducted February through June 1990. It was conducted by OIG's then Office of Security Oversight, which is now the Office of Security and Intelligence Oversight (SIO). The results of that inspection were published in OIG report OSO/I-90-24, dated September 1990.

Although DS as a whole has not been inspected since 1990, many DS programs, including those within DS/SI, have since been audited or inspected by OIG, some very recently. For example, the FY 2003 Intelligence Authorization Act (P.L. 107-306, Section 832) requires OIG to review the Department's protection of Sensitive Compartmented Information (SCI) material, one of DS/SI's programs, in three audits conducted in consecutive years, beginning in 2002. The first two of these audits have been completed; the third was in progress at the time of this inspection. Each year's audit examines a different aspect of the protection of SCI material. Those programs of DS/SI that have been recently reviewed, or are currently under review, such as the audit currently underway, were not reexamined during this inspection. A complete list of recent audits and inspections of DS/SI programs, including the SCI audit in progress at the time of this inspection, is provided in Appendix I.

Other parts of DS, with its 22 offices and approximately 2,400 direct-hire employees and 1,200 headquarters contractors, will be reviewed in future inspections.

## EXECUTIVE DIRECTION

Strong leadership has helped DS/SI rapidly achieve the improvements intended when it was established in May 2003. The senior coordinator for DS/SI has put together a strong team of senior managers. Together they have markedly improved three programs that affect every employee in the Department. Security clearances are being processed and managed more efficiently and in dramatically shorter time frames. The rigorous security incident program is receiving high-level attention through semiannual reports from the DS Assistant Secretary to his Department counterparts. Additionally, computer security awareness has been enhanced through widely available and required on-line training programs, while information systems are ever more effectively monitored for intrusions and abuses.

These achievements were not easy to effect. Previous OIG reports had cataloged significant backlogs in security background investigations, uneven processing of security infractions, and laxity in Department computer security.

The senior coordinator and his managers skillfully use metrics to assist in achieving their management goals. In fact, measurement of almost everything quantifiable, including caseloads and response times, is a prominent characteristic of their management style. Metrics are used to identify and resolve problems, measure performance, and set performance goals. Performance measures have been particularly helpful in enhancing accountability, which has helped increase productivity. Better management, for example, has helped greatly reduce the backlog of periodic reinvestigations and nearly 52 percent of security clearances in all categories are processed within 90 days.

Another prominent organizational characteristic is the customer service ethic. The DS/SI leadership's commitment to delivering services in a timely, transparent, and practical manner won widespread praise from end-users throughout the Department. DS/SI was reportedly particularly responsive in quickly processing clearances for contract personnel for Iraq, China, and the G-8 Summit. High-ranking appointees have received similar attention, and DS/SI's new, more succinct format for reporting background investigation results to the White House has facilitated overall processing of Presidential nominees. DS/SI collaboration with the Bureau of Information Resource Management has enabled the Department to certify 94 percent of its general support systems and major applications as meeting federal

security requirements. Almost to a person, OIG interlocutors noted during the survey phase of the inspection that service had improved markedly since the establishment of DS/SI. The recent establishment of a customer service unit in DS/SI/PSS will help to institutionalize the customer service orientation. DS/SI's strong customer service orientation also stems from executive management's understanding of Department and administration policies, goals, and objectives.

OIG found that DS/SI management has energetically pursued the President's Management Agenda goal of "e-government," and examples abound. DS/SI recently deployed a new automated case management system, RMS, which will enable automated passage of background information to appropriate users in the investigative and adjudicative process, with savings in both time and personnel resources. RMS will also aid management in monitoring the clearance process. DS/SI/PSS has created an interface with the Bureau of Human Resource's on-line Intranet site that allows employees to check on the status of their clearances and allows regional security officers (RSOs) overseas to verify clearance information. DS/SI/PSS has started using the Office of Personnel Management's (OPM) convenient Electronic Questionnaire for Investigations Processing (e-QIP) for on-line collection of data from employees for their periodic reinvestigations. The Office of Computer Security's Network Monitoring Center (b) (2)(b) (2) employs over 800 sensors to monitor every part of the Department's domestic and overseas information technology infrastructure for intrusions. DS/SI publishes a daily report of the center's activities, which Department information technology managers find useful.

The senior coordinator set rightsizing as an early and necessary goal, and OIG found he has succeeded. DS/SI has the personnel resources it needs, but the coordinator will need to monitor the issue as he continues to mold the new organization.

The coordinator and his managers are rightly concerned, however, about DS/SI's personnel makeup. DS/SI employs roughly 855 contractors, and in some offices such as the Computer Security Division the ratio of direct-hires to contractors is very low. Although OIG found no particular problems, management is rightly concerned about the span of supervision and also about whether the wide use of contractors could result in a lack of development of in-house expertise in some functions. DS/SI managers rightly intend to monitor this situation and seek additional full-time equivalent (FTE) direct-hire positions if they are warranted.

DS/SI's large number of contractors and the growth of out-sourcing in general also raise other issues on which the senior coordinator and his managers are correctly focused. They are intent on making sure contracts are concluded correctly and used for the intended purposes and not just as "body shops" for additional personnel resources. They also very correctly seek the flexibility to obtain services and personnel in the most prompt and cost-effective manner. Difficulties in reprogramming funds, the restrictive nature of using blanket purchasing agreements, and the time needed to conclude personal services contracts (PSCs) have sometimes led to using more expensive large contractors, or sole source contracts, to meet pressing needs. Although this practice is sometimes justified, management understands that it is not in keeping with either federal acquisition policy or good management. DS/SI is developing a long-term personnel strategy that will help ensure the correct mix of direct-hires and contractors and may include more use of cost-effective PSCs. Also, metrics are being employed to help quantify investigative management activities to make them suitable for acquisition under the equally cost-effective blanket purchase agreements.

OIG found management has done a good job of integrating contractors into the workplace, and there were no apparent significant divisions between direct-hires and contractors. OIG also found no major problems or incidents of contractors engaging in de facto supervision of direct-hire employees, appearing to speak for the U.S. government, or engaging in other inherently governmental functions. Again, however, management recognizes that the growth of outsourcing demands constant vigilance in these areas.

Employees expressed comfort with DS/SI management's attention to Equal Employment Opportunity issues. OIG found the senior coordinator committed to Equal Employment Opportunity goals. He meets monthly with the DS Diversity in the Workplace Advisory Committee.

The senior coordinator works closely with his most senior managers, conscientiously seeking both to address current issues and to help in developing their potential and skills. In addition to a twice-weekly DS/SI office directors meeting, he interfaces regularly with top managers throughout the day. Top managers in turn provide the DS front office with daily snapshots of significant program developments. Senior managers also personally brief the Assistant Secretary quarterly on their program activities. When seeking resources, senior managers must prepare and defend a proposal before their peers at a monthly DS resource board meeting.

OIG found, however, that the senior coordinator needs to provide more regular information and feedback - including some positive feedback - directly to bureau employees. He has clearly communicated his vision, but the establishment of the new office, restructuring, and new initiatives and ways of operation dictate a need for additional, regular communication with employees. In response to OIG's finding, the special coordinator has instituted monthly staff meetings with mid-level managers to provide and seek feedback and has scheduled quarterly all-hands meetings for the same purpose. He is also putting together an e-mail collective to assist in providing employees regular information. Finally, DS/SI is reinvigorating its awards program.

OIG found morale to be generally good, and it shows signs of getting better as employees become accustomed to the new organizational structures, new software, and the use of metrics and resultant increased accountability. There is widespread respect for the senior coordinator and his accomplishments.

Senior DS/SI managers recognize the importance of training, and the new customer service unit has been tasked with developing some much needed training initiatives. The senior coordinator is personally involved in developing in-house training on drafting skills that can be tailored to DS/SI's specific needs.

The DS Bureau Performance Plan provides comprehensive detail on DS/SI's activities, needs, and plans and links them to resources and resource needs. The senior coordinator and his top managers have also worked carefully with DS/SI's budget. Fulfilling an earlier OIG recommendation, the background investigations budget is now well focused, sufficient, and more transparent.

DS/SI's jump in productivity and its strong focus on customer service led some employees to raise questions of whether quality might be sacrificed for quantity. DS/SI will need to monitor operations closely to assure this does not happen. Establishment of a new quality assurance unit in DS/SI/PSS is a step in the right direction.

On internal management controls in general, the results of risk assessment questionnaires showed that due to the nature of its functions, DS/SI is in the moderately high-risk category for susceptibility to fraud, waste, and mismanagement. The risk can be minimized through an operating environment that supports good management controls, and scores indicated that DS/SI controls are good, with the exception of some weaknesses in DS/SI/PSS (detailed in the DS/SI/PSS section of this report).

## POLICY AND PROGRAM IMPLEMENTATION

### OFFICE OF PERSONNEL SECURITY AND SUITABILITY

DS/SI/PSS has markedly improved its productivity, responsiveness, and customer service since the establishment of DS/SI. DS/SI/PSS has brought the average processing time of a security clearance down from 195.2 days in 2003 to 118.7 days thus far in 2004. Presently, 52 percent of clearances are completed in less than 90 days. Periodic reinvestigations of employees have been automated. An initiative expanding the use of interim clearances has put people to work faster. Plans to restructure the office should result in additional improvements. DS/SI/PSS's goal is to complete 75 percent of its applicant cases within 90 days in FY 2005 and subsequent years.

DS/SI/PSS is charged with assuring that granting an individual access to classified information is consistent with the interests of national security. The Department is one of the few U.S. government agencies that continue to perform its own background investigations, and DS/SI/PSS conducts background investigations and adjudicates clearances on applicants, current employees, and sometimes on contractors. It works with the Defense Industrial Security Clearance Office (DISCO) on the majority of contractors. The Adverse Action Division makes security clearance suspension and revocation determinations. DS/SI/PSS has a staff of 130 direct-hire and contract employees and more than 600 contract field investigators throughout the United States. Its budget is \$20 million. DS/SI/PSS conducts about 20,000 investigations annually to standards set by Executive Order.

The DS/SI/PSS office director came to the Department about five months ago, but brought with him a career of experience in the personnel security field. OIG found he has already developed a comprehensive grasp of the Department's personnel security program, and he is earning the respect and confidence of his staff.

DS/SI/PSS currently consists of four divisions: Applicant Investigations, Adjudications, Periodic Reinvestigations, and Adverse Actions. However, the office intends to reorganize in 2004 into a new configuration consisting of two

mirror-image divisions of investigator/adjudicator teams, the Adverse Actions Division and a new Customer Service Division. (A customer service unit has already been created. See below.) The reorganization is the result of a study by DS/SI managers and the recommendations contained in a 2003 report by a contractor on the security clearance process. DS/SI/PSS will consolidate the investigations case managers and adjudicators into joint teams. DS/SI/PSS believes having adjudicators perform case management functions will be a force multiplier, and will also incorporate the adjudicative expertise at the beginning of the investigation, rather than the end. The change should also promote a more equal distribution of work and foster greater ownership of cases. The establishment of a formalized structure for customer service will help institutionalize this important aspect of the office's work. OIG agrees that the reorganization should further increase both productivity and the quality of work.

A small interim clearance coordinator's (ICC) office was established outside the four office divisions in October 2003 to expedite the issuance of interim clearances to permit newly recruited employees to begin work quickly. It has proved a success. The office's procedures, consistent with E.O. 12968, are designed to identify applicants without significant security risks and to grant them interim clearances. For secret clearances, the office's staff review the applicants' responses to the questions on form SF-86, which relate to citizenship, military record, medical matters, drug and alcohol use, criminal record, and financial problems, among other things. If there are serious, unresolved issues in these areas, the ICC does not grant an interim clearance and informs the requesting office of that decision. The process is similar for requests for Top Secret clearances, but in those cases, the ICC also conducts a National Agency Check. From October 2003 until the end of August 2004, the ICC has granted 2000 interim clearances and has denied 599 requests for interim clearances.

A customer service unit was established in November 2003 to handle all inquiries into the status of cases from within the bureau and the Department (and therefore by extension from Congress, the White House, and other outside entities). The unit also helps RSOs in the field, manages DS/SI/PSS orientation and training, facilitates DS/SI intra-office communication, troubleshoots RMS, and is the point of contact for e-QIP and with all other agencies. It is managed by an experienced direct-hire employee and is composed of five contract personnel, four of whom were formerly case managers. Like the interim clearance unit, the customer service unit currently lies outside the office's four divisions. However, after the reorganization, it will be part of the customer service office.

DS/SI/PSS has a number of additional functions. It develops the Department's policy and procedures on security clearances, which are published in the Foreign Affairs Manual. It also assists in the interpretation and application to the Department of Executive Orders pertaining to the conduct and adjudication of security clearances.

DS/SI/PSS maintains close and effective liaison with other agencies. The ICC and certification unit within DS/SI/PSS routinely works with other agencies in granting reciprocal clearances and in passing on information on the security clearances of traveling officials from those agencies to Foreign Service posts around the world. DS/SI/PSS works particularly closely with OPM, which now processes clearances for most U.S. government agencies, and the Department employs OPM's e-QIP for on-line collection of data from Department employees for their periodic reinvestigations. A three-person liaison team maintains contact with the Department of Defense, the Central Intelligence Agency, the FBI, the Defense Intelligence Agency, and other agencies. DS/SI/PSS has assigned one person to the FBI to ensure speedy action on the FBI checks required for security clearances.

DS/SI/PSS also plays an active role in the interagency personnel security community. The senior coordinator sits on the Committee on National Security Systems and frequently represents DS at the Intelligence Community's Security Directors Forum. DS/SI/PSS is closely engaged with the National Security Council Subcommittee on Personnel Security.

Interagency contacts keep DS/SI/PSS aware of trends and developments in the personnel security community. Top DS/SI/PSS managers have visited OPM's security clearance center in Pennsylvania and are impressed with its organization, automation, and capabilities. DS managers are studying the possibility of additional use of some of OPM's capabilities and services but believe that the Department's program's current effectiveness, and the need for the flexibility to sometimes intervene and prioritize cases, justifies the need for DS to continue to do investigations and adjudications. OIG agrees.

The results of the risk assessment questionnaire disclosed several areas of weakness in internal management controls. The office is reliant on outside contractors, including sole source contracts. Management must therefore be attentive to the outsourcing concerns catalogued in the Executive Direction section of this report. OIG found that the new office director is well aware of potential weaknesses and has developed new contracting strategies, such as the use of PSCs and the acquisition of more direct-hire FTEs, which should adequately address concerns.

This risk assessment also pointed out the need to review and update position descriptions. This will be particularly important given the pending reorganization.

**Recommendation 1:** The Bureau of Diplomatic Security should review, and update as required, all position descriptions in the Directorate of Security Infrastructure, Office of Personnel Security and Suitability. (Action: DS)

OIG observations and the risk assessment questionnaire also identified a need for improved and continual training in the investigative and adjudicative functions. The lack of a formal training program and the number of new employees make this imperative. OIG informally recommended development of a training program. Management was responsive and has tasked DS/SI/PSS's new customer service unit to develop a training plan.

OIG found the new office director correctly focused on improving both vertical and horizontal communication in DS/SI/PSS. The pending reorganization and establishment of a formal training program should facilitate this effort.

The office's size, intense workload, and vulnerability to lapses in internal management controls present a supervisory challenge to whoever occupies the office director position. This might be alleviated by creation of a deputy director position such as those found in much smaller offices. OIG informally recommended that the bureau's executive office review the DS/SI/PSS organizational structure and supervisory span of control.

### *Periodic Reinvestigation Division*

The Periodic Reinvestigation Division is effectively accomplishing its primary function, which is to conduct periodic reinvestigations on all Department employees. Executive Orders require that these reinvestigations be done every five years.

Improvements in the performance of the division's function are seen in two areas. First, the division has reduced its backlog of open cases from 6,114 in FY 2002 to 1,105 in FY 2004. Second, there has been improvement in the length of time needed to close cases. The performance standard for the division is to close cases within 90 days. In FY 2002, only 25 percent of cases were closed within 90 days, but in FY 2004 over 51 percent of cases were closed within 90 days. These

improvements occurred at the same time the PR division assumed additional responsibility for the investigation of Presidential appointees, contractors considered for work in Iraq and Beijing, and a number of other special categories of personnel requiring clearances.

The Periodic Reinvestigation Division is also trying to develop a workable solution to its biggest problem - overseas reinvestigations. The Department's RSOs are responsible for overseas investigations. Response to investigation requests has sometimes lagged as RSOs have become increasingly engaged with protection of life, information, and facilities. RSOs currently take an average of 113 days to complete an overseas investigation. This appears to be an improvement over about 138 days a year ago, but continued improvement is obviously imperative to meet DS/SI/PSS's 90-day clearance processing standard.

To improve their performance and the percentage of cases closed within 90 days, the division has assisted in the development of two new information technology programs that are very promising. The RMS is a web-enabled application designed to improve the service time of investigations and reduce case backlog. The RMS system gives managers the ability to monitor employee performance. The result is increased employee accountability. The other initiative is use of the OPM e-QIP. The e-QIP system is an automated database that allows employees to fill out security forms via the Internet. One benefit of this system is that electronic data entered into e-QIP can be downloaded into the RMS system.

The improvements in performance have been accomplished with a staff of 16 direct-hire employees working under the direction of a new management team. The division also uses 12 contractors to supplement its staffing. The staff complement is sufficient, and no additional positions are needed at this time. Nonetheless, additional direct-hire employees could be needed if the demand for investigations increases. Although employees have undergone several reorganizations and will experience another in two months, morale within the office is uniformly good. Contractors are adequately supervised and they do not perform functions such as granting security clearances or supervising government employees, which are inherently governmental, nor do they influence governmental policy. The ratio of direct-hires to contractors is appropriate.

### *Adjudications Division*

The Adjudications Division reviews the 20 percent of background investigations that contain information that could lead to denial of an employee security clearance. Headed by a GS-14 division director, the unit's two GS-13 unit chiefs

manage a staff of 12 personnel security specialists and two contractors. Morale is high in the division, and division employees bring many years of adjudicative expertise to the office.

Like the rest of the DS/SI/PSS, the Adjudications Division has been asked to address a number of special “surge” projects, ranging from new hires for the Diplomatic Readiness Initiative to contractors for Embassy Beijing to Iraq-related hiring, all on short-fuse deadlines. Presidential appointments, investigated by the FBI but adjudicated by the Department, require expedited handling in coordination with the Adverse Actions Division. Each of these challenges has been met effectively with existing staff. The workload of 132 cases is manageable; there is no backlog of cases awaiting adjudication.

In applying federal adjudicative guidelines, DS adjudicators weigh a number of variables to arrive at decisions, a process known as the “whole person” concept. Facts in each case must be considered on a case-by-case basis, and adjudication frequently involves referrals to the Office of Medical Services, Civil Service and Foreign Service suitability panels, and other offices within DS. The process is inherently labor and time intensive. OIG found in a review of adjudicated files that managers generally addressed relevant issues prior to issuing clearances. Files were promptly adjudicated in nearly all cases examined. Nevertheless, some files contained derogatory information that was not always noted by the adjudicator, particularly in the area of financial responsibility. Files are not reviewed by a supervisor as frequently as they should be. Each adjudicator maintains an individual file tickler system, but there is no system in the division for supervisory reviews of files at regular intervals.

Based on a recommendation from a management consultant in 2003, DS/SI/PSS intends to implement a major reorganization of the adjudicative function. The pending reorganization of DS/SI/PSS will abolish the Adjudications Branch, resulting in the transfer of current staff to the Applicant and Periodic Reinvestigation Divisions. The reorganization offers advantages and disadvantages. The proposed reorganization eliminates a layer of review that, at present, leads to delays in processing files. Several adjudicators noted that approximately 10 percent of files must be referred to the applicant or periodic reinvestigation units for expanded investigations. Investigations destined for a security clearance denial must sometimes be referred to four offices within DS/SI/PSS before a final security clearance decision is made. The reorganization should eliminate these problems, as case managers will be responsible for both investigation and adjudication of the personnel investigation.

What one manager described as “reorganization fatigue” is a real factor: the Adjudications Division was only created two years ago and is now being abolished. Employee buy-in for the reorganization does not yet exist. To ensure that the current reorganization succeeds, management must explain clearly the rationale for the reorganization to employees. Many adjudicators have little experience managing investigative cases. As a result, they are not familiar with investigative operating procedures and computer systems. Adjudications staff need training on the Case Management System (CMS) and RMS computer systems - not heavily used by adjudications staff at present - as well as training in investigative case standards. Also needed are standard operating procedures for the new office to clearly delineate responsibilities. Clear communication from management during this change is particularly important with respect to application of performance metrics that may be unfamiliar to most adjudications staff. OIG counseled division management to hold regular all-hands meetings to keep employees abreast of changes required by the reorganization and to assess its progress.

The nature of the adjudicative function does not lend itself to quantifiable performance metrics. Currently, adjudicators are expected to perform three referral actions a day - either approval of a clearance or referral of the file to another office. This performance measure is not yet used by management to track the performance of individual adjudicators. When the new quality assurance office is set up, DS/SI may want to institute qualitative metrics to evaluate adjudications. Because of a lack of performance and workload metrics, it is difficult to determine whether staffing for the division is appropriate.

In 2000, the Adjudications Division acquired responsibility for handling most aspects of the Department’s SCI clearances. Two adjudicators work on 1,400 SCI clearances annually, including renewals of clearances. The SCI workload is burgeoning, according to DS management. DS prepares adjudications reviews for SCI clearances, but the senior official of the intelligence community in the Bureau of Intelligence and Research makes the final adjudicative determination of eligibility, in most cases mirroring the decisions made in the Top Secret adjudication.

### *Background Investigation Quality Assurance*

In 2001, OIG conducted an in-depth review of 50 adjudicated security clearances as part of an audit of the background investigation process.<sup>1</sup> Federal standards under Executive Order 12968 require that background investigations address

---

<sup>1</sup> *Audit of the Department’s Background Investigations (01-SIO-R-061).*

nine elements: birth and citizenship, education, employment, residences, reference checks, national agency checks, local agency checks, credit history, and a personal interview. The 2001 OIG audit found deficiencies in a variety of investigative elements required by the standards. The chief areas of weakness were national agency checks (96 percent deficient), employment verification (46 percent deficient), and local agency checks (40 percent deficient).

OIG revisited the security clearance process by conducting a second in-depth review of 51 adjudicated files during the inspection. Results of this review indicate that DS has made significant progress in addressing some investigative deficiencies. For example, nearly all files examined in 2001 lacked FBI investigative file information. Transfers of FBI data are now automated, a change that appears to have increased accuracy in performing national agency checks. Only two files lacked FBI investigative information in 2004. None lacked FBI name checks, OPM, or Department of Defense database checks, in part because DS now has direct access to most of these agencies' databases. The Central Intelligence Agency and Department of Homeland Security databases are not automated, however, leading to a higher noncompletion rate for these critical functions. Continued automation of the national agency check function remains one of DS management's priorities.

However, some significant deficiencies in investigative quality remain to be addressed. (See Figure 1 below.) Local agency checks were not completed in 37 percent of cases; national agency checks were not completed in 29 percent of cases; and employment verification was not obtained in 18 percent of cases. Only

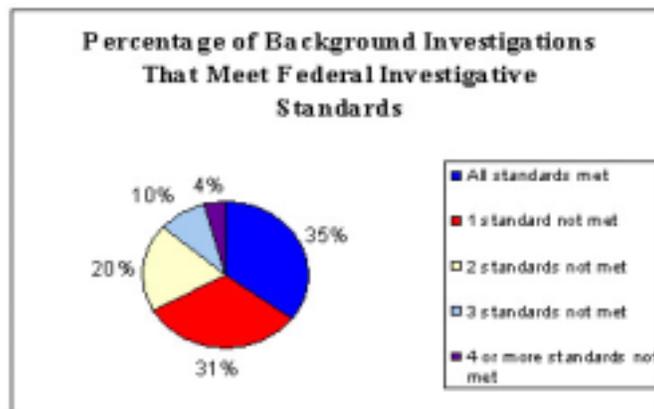


Figure 1 - Percentage of Background Investigations That Meet Federal Standards

31 percent of files met all investigative standards appropriate to the class of investigation.<sup>2</sup> Deficiencies in national agency checks are especially relevant to the interim clearance process, in which an interim clearance is granted primarily on the basis of records checks. These weaknesses have potentially serious implications for national security.

OIG believes that file quality could be improved by a four-pronged approach that integrates quality measurements into the bureau's performance goals. The most important step is to institute a formal quality assurance unit that continually evaluates case files. At the time of this inspection, DS was in the process of hiring three individuals to staff such a unit, and duties for the unit had not been defined. The second step is to institute an in-house training program for investigators and adjudicators. The third is to ensure regular supervisory review of investigative and adjudicative files. The fourth step is to automate national data checks to the greatest extent practicable, particularly with respect to fingerprints, where significant vulnerabilities exist. These issues are discussed in greater detail below.

### *Fingerprint Checks*

In OIG's view, the most pressing area of deficiency in the investigative process is continued difficulty in completing FBI fingerprint checks for new applicant investigations. A check of FBI fingerprint records is required under Executive Order 12968 to cross-reference felony arrest records. DS now uses a combination of electronically scanned paper fingerprint cards and digital fingerprints to obtain records. The process sometimes yields fingerprints that are not readable by the FBI's system for a variety of reasons. FBI electronic responses must be manually matched to individual case files, a time consuming and error prone process.

When a fingerprint check is inconclusive, investigative files contain little evidence that case managers follow up to obtain new prints from applicants. Of the sample reviewed by OIG, 16 percent of cases did not have conclusive fingerprint information on file from FBI. Inconclusive fingerprints increase the possibility that individuals who are risks to national security could obtain clearances. OIG believes that in addition to reiterating to case managers the importance of fingerprint checks, DS management should institute internal controls in future versions of RMS and CMS to prevent closing a file when fingerprints have not been identified. Enhancements to improve matching FBI data to CMS records should also be considered.

---

<sup>2</sup> OIG examined only the most recent background investigation in the sample for Single Scope Background Investigation - Periodic Reinvestigation cases, rather than all prior investigations in the file. Data for most measures are not directly comparable to the 2001 audit data.

**Recommendation 2:** The Bureau of Diplomatic Security should institute internal controls to ensure that conclusive Federal Bureau of Investigation fingerprint results are obtained for all applicant investigations and matched to the appropriate investigative files. (Action: DS)

### *Supervisory Review*

Supervisory review is a primary management control tool for ensuring that clearance decisions meet federal standards. Five separate units in DS/SI are authorized to grant security clearances: the interim clearance unit, the investigations unit, the periodic reinvestigations unit, the adjudications unit, and the adverse action unit. Each unit applies different standard operating procedures and uses different forms in granting security clearances. However, supervisory review of files does not occur on a systematic basis in most units in the division. The final decision to grant a clearance was not reviewed by supervisors in 43 percent of cases examined by OIG. Particularly with interim clearances, supervisory review is an internal control necessary to prevent individuals who are security risks from being granted clearances.

**Recommendation 3:** The Bureau of Diplomatic Security should establish procedures to verify that all background investigation files are complete and meet federal standards prior to the final decision to grant a security clearance. (Action: DS)

### *Adverse Actions Division*

OIG found the Adverse Actions Division handles suspensions and revocations of security clearances with the professionalism merited in such a sensitive function. Interlocutors in the Bureau of Human Resources and other parts of the Department lauded the personnel security specialists and the experienced division director for their thoroughness, responsiveness, and balance. Interviews of the specialists and reviews of cases corroborated this judgment.

The 13-person Adverse Actions Division staff is composed almost entirely of senior GS-13 personnel security specialists. The specialists evaluate security clearance eligibility in light of reports documenting alleged or substantiated conduct that indicate an employee's continued access to classified information may not be in the interest of national security. The reports of derogatory information are

most often provided by the DS Office of Investigations and Counterintelligence, but referrals also come from the Office of Periodic Reinvestigations, OIG, the Office of Passport and Visa Fraud, the Bureau of Human Resources' Office of Employee Relations/Conduct and Suitability Division, the DS/SI Application Programs Division, which handles the security incident program, and other personnel security operations within the federal government. OIG refers suitability issues to DS when they arise as part of an OIG investigation or are referred to OIG by way of the OIG Hotline.

The personnel security specialists first determine whether suspension - a temporary measure - is warranted, and processes the suspension. The specialists next evaluate the allegations and investigation results in context of the employee's overall security file and history and in accordance with National Security Council adjudicative guidelines. They then make a recommendation to the Director of the Diplomatic Security Service (DSS) (who serves concurrently as DS principal deputy assistant secretary) to revoke or reinstate the clearance. The detailed recommendations contain case summaries and analyses, including mitigating circumstances or extenuating circumstances. An OIG review of select cases showed them to be well developed and balanced in keeping with the "whole person concept" laid out in the DS Personnel Investigation Procedures handbook.

The DSS director's decision can be appealed to a panel consisting of the Under Secretary for Management, the Assistant Secretary for Administration, and the Director General. The panel will probably hear about six cases this year.

The division manages an average caseload of 30-35 suspensions/revocations (currently 41). It monitors another 150 cases of employees under investigation, medical treatment/review, or sanctions for drug use. Under a positive new initiative, suspended cases are reviewed daily in order to ensure they are resolved as expeditiously as possible. Management strongly believes quick resolution to be in the interests of both the employee and the U.S. government. However, resolution is often delayed by the need for additional investigation and by the submission of additional input by the subject employees and their representatives.

The division is also the single point in DS for vetting candidates for promotions and tenure, D-Committee appointments and assignments and high-level awards, using database checks and file reviews. Bureau of Human Resource officials roundly appreciated the division's thorough, accurate, and expeditious handling of these responsibilities. Finally, the division shares responsibility for adjudicating Presidential appointments and preparing summaries of the investigations for the White House. The Department's Presidential appointments staff was particularly

appreciative of a recent new formatting initiative by the Adverse Actions Division that has made the reports more concise and facilitated more rapid overall processing of nominees.

Given these responsibilities and the often lengthy, complex, and labor-intensive nature of suspension and revocation cases, the average caseload of about 20 cases per employee appears appropriate, and the division appears to be the right size.

OIG found the Adverse Actions Division to be well managed. Employees appreciate the division director's clear direction, individual attention, and organizational abilities. The division was one of the first divisions to complete a standard operating procedure, drafting it as a team exercise. The division also regularly "teams" difficult or unique cases, which not only facilitates case resolution but also provides training and promotes employee development. Weekly staff meetings assure continuous vertical and horizontal flow of information and feedback.

Some Department interlocutors during the survey phase of the inspection noted that the creation of the security infrastructure directorate had added additional layers of review in the processing of cases en route from the division to the DSS Director, delaying case resolution. DS acknowledged the problem and is addressing it by further limiting the number of reviewing officials, standardizing and enhancing case formatting, and drafting and introducing more oral presentations of cases to the Director of DSS by the personnel security specialists.

Adverse action cases are not entered into division databases such as RMS and CMS due to privacy considerations. Status and management reports must be compiled from Microsoft Word files, largely denying the Adverse Actions Division the benefits of automation. While the number of cases handled by the division is not large at any one time the numbers mount up over time, and automation would enhance both accountability and productivity. It may be possible to define an adverse action role in RMS that would allow only the Adverse Actions Division staff to access adverse action cases. This would protect the privacy of employees and also provide the division the benefits of RMS automation. OIG informally recommends further study of this issue.

### *Applicant Investigations Division*

OIG found the Applicant Division works increasingly effectively to process a large volume of security background investigations. The division has been facing challenges of growing caseloads, shorter processing time frames, and new computer software. In spite of these challenges, morale is high.

The Applicant Division was established in October 2002 as a result of the latest of several reorganizations. It moved in its current form into DS/SI in May 2003. Its main function is to conduct background investigations on all new employees and PSCs within the Department. If investigation results indicate no problems, the case managers adjudicate the case and a clearance is issued. If an investigation raises questions meriting further study, the case is sent to the Adjudications Division. The division also serves as the primary interface with DISCO and the Defense Security Service, which investigate and process clearance requests for Department contractors. The division now consists of ten direct-hire and 17 contractor employees in Washington headquarters and hundreds of contract investigators in the field.

DISCO's and the Defense Security Service's large backlog, and the need to get Department contractors to Iraq and Beijing, has necessitated the Applicant Division's taking over responsibility for some contractor clearances. This has enabled the Department to get these contractors to work more quickly.

Case managers review and assign cases to the background investigations coordinator at a field office. The coordinator assigns cases to contract investigators. Attempts are made to keep caseload per case manager at 150. However, increased demand, such as hiring under the Diplomatic Readiness Initiative and the decision to undertake some contractor cases, has meant higher caseloads with some managers having had as many as 254. This necessitated hiring contractors to augment regular case managers' efforts, and OIG found that this has helped significantly. The caseload, however, is still heavy and introduction of the new RMS software has added an additional data-entry burden.

The division's goal is to process all cases, except for Presidential nominations, within 90 days. Presidential cases are to be completed in 30 days. Special cases, such as the contractors for Iraq, are processed within 14 days. The division's caseload is currently 3,323 cases, of which 1,819 cases are past the 90-day mark. A portion of the cases was recently transferred to the Periodic Reinvestigations Division, which had a smaller number of cases.

The Applicant Division also manages and passes requests for overseas background investigations from the Department of Defense, OPM, and other agencies to RSOs in the field. Responses from RSOs to these requests sometimes lagged due to competing priorities, but requests for more responsiveness from DS management to RSOs on this issue has improved the situation.

Plans to amalgamate the Applicant Division with the Periodic Reinvestigations and Adjudication Divisions into two divisions of investigations/adjudications teams should alleviate the heavy caseload and more equitably distribute the DS/SI/PSS workload, helping DS/SI/PSS meet its rightsizing goal.

OIG reviewed 50 randomly selected background investigations. The results of this review are described in the Background Investigation Quality Assurance section, Adjudications Division, of this report.

OIG found that training has been performed on an ad hoc basis and does not appear to meet adequately the needs of the staff. Several employees expressed concern about the lack of standardized training. A review of randomly selected case files showed that some files were not properly processed, indicating a need for refresher training and greater attention to detail. The division is working to address this matter and some refresher training has been provided. However, more is needed, and OIG has informally recommended the establishment of a DS/SI/PSS-wide training program.

## OFFICE OF COMPUTER SECURITY

The Office of Computer Security provides sound security support to the Department's information technology infrastructure through a monitoring, regulatory, and analytical program. However, OIG found several areas requiring management attention. These include a lack of standard operating procedures and performance measures for the regional computer security officer (RCSO) program, and the need to coordinate RCSO activities with the Office of Information Assurance.

DS/SI/CS consists of four divisions: the Detection and Analysis Division, the Systems Standards Division, the Risk Assessment Division, and the Global Support Division. The Detection and Analysis Division is responsible for the operation of the intrusion detection, computer incident response, and cyber threat analysis cell programs. The Systems Standards Division is in charge of developing, maintaining, and interpreting information systems security policies in the 12 FAM 600 series and 12 FAH-6. The Risk Assessment Division is responsible for security analysis, including the development of security configuration guidelines for hardware and software and the management of the baseline toolkit used to check the configuration guidelines. The Global Support Division is in charge of computer security awareness and the RCSO program. The Office of Computer Security's practice of

hiring numerous contractors has given it the staff needed to perform the work of the organization. DS/SI/CS is thus rightsized. The unit's practice of outsourcing is in accordance with the President's Management Agenda.

OIG found that DS/SI/CS employees and contractors are skilled and well trained. Many of them hold the A+ and the Microsoft certified systems engineer certifications. The Detection and Analysis Division has developed standard operating procedures for the computer incident response program and intrusion detection programs. The division also provides a daily cyber security briefing providing statistics on patch management, intrusion attempts, and computer security incidents. OIG found, in this and in previous inspections, that the intrusion detection program works well. Additionally, the Global Support Division developed an online training application to meet agency-wide computer security awareness training requirements.

Regarding internal management controls, the results of the risk assessment questionnaire revealed that the office has a moderately high inherent risk, largely attributable to the nature of its work. Such risks can be largely mitigated by good management controls, and the scores of the questionnaire revealed that DS/SI/CS has good controls.

### *Regional Computer Security Officer Program*

OIG found that the Global Support Division has not developed standard operating procedures for the RCSO program. Regional computer security officers are responsible for ensuring that the classified and unclassified networks are installed and maintained according to current Department and U.S. government security regulations. They provide onsite computer security customer support, training, and independent evaluations of unclassified and classified networks. Towards that end, DS officials told OIG that a common practice included running the baseline toolkit to ensure compliance with the Department operating system guidelines. What is lacking, but according to DS personnel is under development, are formal written procedures for the conduct of site verification and evaluations conducted either by RCSOs or headquarters staff.

**Recommendation 4:** The Bureau of Diplomatic Security should develop and implement standard operating procedures for the activities of the regional computer security officer program. (Action: DS)

OIG also found that DS has not developed performance measures to evaluate the effectiveness of the RCSO program. Performance measures can assist in evaluating the success or failure of an agency program. DS officials did, however, provide OIG with some annual site visit goals, but the results of the visits are not part of this measure. Other DS officials told OIG that the organization is working on developing some metrics, but currently, formally documented performance measures do not exist. The lack of adequate performance measures could result in ineffective use of the RCSO program funds.

**Recommendation 5:** The Bureau of Diplomatic Security should complete the development of and implement appropriate metrics to measure the performance of the regional computer security officer program. (Action: DS)

(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)  
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)  
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)  
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)  
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)  
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)  
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)  
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)  
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)  
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)  
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)  
(b) (2)(b) (2)

**Recommendation 6:** (b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)  
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)  
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)  
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)  
(b) (2)

<sup>(b)</sup> (b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)

## OFFICE OF INFORMATION SECURITY

DS/SI/IS is largely meeting its program objectives. Since its incorporation into the Directorate of Security Infrastructure, DS/SI/IS has undertaken many new initiatives to better support the Department and the needs of its customers. Its elevation from division to office status has given needed higher profile to its programs. Combining DS/SI/IS under one directorate with the offices of personnel security and suitability and computer security has facilitated the sharing of information on crossing-cutting issues.

DS/SI/IS has three divisions: Special Security Operations Division, which ensures compliance with Director of Central Intelligence Directives (DCIDs) for the protection of SCI and other intelligence; Industrial Security Division, which oversees the Department's industrial security program; and Program Application Division, which manages the protection of classified and SBU information within the Department. In addition, the office has a special projects unit, staffed by contract and direct-hire employees, who report directly to the office director. DS/SI/IS is staffed by 42 direct-hire employees and 48 contractors, who are located in the Harry S Truman (HST) building, SA-20, and at the Navy Hill Annex, SA-4C.

A key focus of DS/SI/IS's support of Department programs has been its assistance to Embassies Baghdad and Kabul, which has been in several key areas. With DS/SI/IS's assistance, sensitive compartmented information facilities (SCIFs) to support Ambassadors Negroponte and Khalilizad have been certified and accredited. DS/SI/IS has designed and implemented life-safety tracking devices with sophisticated monitoring capabilities and has assisted DS protective operations. Domestically, DS/SI/IS has supported the Bureau of Overseas Buildings Operations and DS in analyzing procurement documents and developing security requirements for contractors supporting Baghdad and Kabul. This support has been ongoing, supporting the transfer of responsibilities from the Coalition Provisional Authority to the Department.

Recent DS/SI/IS initiatives have included a snapshot review of 443 firms and 11,422 records to verify personnel security requirements of firms involved in classified and SBU contracts with the Department. Additionally, reviews of 205 small business firms performing classified and SBU contracts to ensure compliance with contract requirements were done. Semiannual reporting of bureau, post, and tenant agency security incident statistics to all assistant secretaries and tenant agency senior officials to bring greater attention to the need to properly handle,

store, and process classified information and the transfer of the Department's SCI access database to the intelligence community's database to facilitate easier access to an individual's SCI access clearances were other initiatives implemented by DS/SI/IS.

### *Management*

On internal management controls, the results of the risk assessment questionnaire revealed that the office has a moderately high risk, and although some areas could be strengthened, overall controls are good. Areas that contributed to the moderately high-risk assessment were dependency on outside contractors, activities and programs that warrant special attention, and significant program changes within the past two years. The office director is aware of these potential weaknesses and is developing strategies to mitigate them.

An area of management concern is the office director's span of control. In addition to the office's three divisions and their respective division directors, the office director directly supervises 13 contract and direct-hire employees. Most of these 13 are part of the office's special projects unit. This unit has a diverse portfolio, including special access programs, foreign diplomat exchange programs, damage assessment, coordination of DS critical infrastructure protection requirements, and SCI and special access programs system certification and accreditation. While there is no universal consensus of the number of subordinates that a manager can effectively supervise or proper amount of centralization/decentralization for an organization, elevating the special projects unit to division status, with a division director, or dispersing its functions among the office's three existing divisions would enable the office director to devote less time to direct supervision and more time to the management of the office.

**Recommendation 7:** The Bureau of Diplomatic Security should reorganize the Office of Information Security to reduce the span of control of the office director and reduce the number of functions and activities that are directly supervised by the office director. (Action: DS)

### *Special Security Operations Division*

Although hampered by crowded, dispersed office spaces, the Special Security Operations Division has made commendable progress in controlling and protecting

the Department's SCI material and in accrediting SCIFs. Additionally SSI has been very responsive to the needs of its customers.

A 1999 OIG audit<sup>4</sup> found that the Department was substantially not in compliance with DCID requirements for the protection of SCI material. Subsequently, the responsibility for protecting SCI material within the Department was transferred from the Bureau of Intelligence and Research to DS, and within DS, to the Special Security Operations Division. This transfer was done incrementally, being fully implemented in 2002. Beginning in 2002, OIG began a series of three annual audits of the Department's protection of SCI material, each focusing on different DCID requirements. The first two of these audits have been completed,<sup>5</sup> and the third and final audit was in progress at the time of this inspection. Although these audits have identified some areas where additional improvements can be made, on the whole they have found substantial improvement in the protection of SCI material and in the accreditation of SCIFs. The audit conducted during 2002, for example, reported that DS had recently implemented procedures for controlling accountable and nonaccountable SCI documents in accordance with DCID requirements. The 2003 audit found that DS had employed an effective process for accrediting SCIFs according to DCID requirements and had established effective programs to ensure that accredited SCIFs and SCIF procedural security requirements are continually met.

The division director and branch chiefs of the Special Security Operations Division have also done an excellent job of adapting the division's programs and activities to best serve the needs of its customers - Department officials who have the need for access to SCI material. The document control branch, for example, has expanded their hours of operation, through overlapping shifts, to serve better early arriving and late departing Department officials. They have also increased the frequency of daily deliveries to get critical information to senior officials in a more timely manner. Employees from the operations support branch have uploaded the Department's SCI access database to the Central Intelligence Agency's intelligence community database. This eliminates the possibility of Department officials being denied access to another agency's SCI-level briefing because their clearances were not passed.

With minor exceptions, the division staff of 18 direct-hire employees and four contractors appears to be rightsized for the division's programs and activities. The document control branch has three vacant contractor positions, which need to be

---

<sup>4</sup> OIG report SIO/A-99-46

<sup>5</sup> OIG reports SIO/A-03-30 and SIO/A-04-11

filled, but as discussed below, there is not adequate space for the existing staff. The operations branch has a need for an office administrator, but because of the shortage of space at its present location, any staff increases should be held in abeyance until the office is relocated to a larger facility.

### *Working Conditions*

The Special Security Operations Division's three branches are at separate locations in crowded conditions that adversely affect the staff's ability to perform their missions. The division director and the Procedural Security and Accreditation/Oversight Branch are located at SA-4C, Navy Hill, across 23rd Street from the HST building. Although the branch has adequate office space at SA-4C, its location physically separates the division director from the other two branches located in the HST building, making supervision and oversight more difficult.

The Operations Support Branch is located in room 2237 in the HST building. The Operations Support Branch staff in room 2237 work under extremely crowded conditions, and the office has no facilities for security briefings, which are a key part of the branch's program. There are plans to relocate the branch to room 2239 in mid-2005, which will provide adequate working space and a briefing room.

Document Control Branch personnel also work in extremely crowded conditions. They're located in the Bureau of Intelligence and Research's 6510 Suite in the HST building, which they share with that bureau's staff. The rooms within the suite that have been allocated to the Document Control Branch are too small for the staff of eleven contract and direct-hire employees. As a result, there are desks for only approximately half of the staff. This is ameliorated by the assignment of branch personnel to overlapping shifts to provide coverage from 4:30 a.m. to 9:45 p.m. Nevertheless, the Document Control Branch staff must share desks, and during the overlap period between shifts some personnel have no place to sit. Also, a major function of the branch is making classified, limited-distribution documents available for reading by senior Department officials. For this function, the branch has only one very small reading space. Some officials have complained about the lack of adequate reading facilities.

**Recommendation 8:** The Bureau of Diplomatic Security should, in coordination with the Bureau of Administration and the Bureau of Intelligence and Research, develop and implement a plan to relocate all personnel of the Special Security Operations Division, Office of Information Security, into the Harry S Truman building and to provide additional office space for the division's document control and operations support branches. (Action: DS, in coordination with A/OPR and INR)

*Industrial Security Division*

As the Department and other federal agencies move towards outsourcing/ privatizing, individual contractors and private firms are assuming a greater role in national security work. The Industrial Security Division, which oversees the industrial security program, plays a key role in this process. The division assists sponsoring bureaus or offices in developing security requirements for contractors that require access to classified or specific categories of SBU information. This includes analyzing procurement documentation, developing appropriate security requirements, establishing education and training programs to ensure contracting officer's representatives (CORs) and facility security officers are cognizant of their responsibilities, conducting security oversight and compliance reviews, verifying contractor facility and personnel security requirements, and certifying contractor requirements for connectivity to Department information systems. The Industrial Security Division facilitates the granting of contract security clearances but does not adjudicate or grant security clearances.

The industrial security program was established in 1986<sup>6</sup>, and the current division director has served as the head of the program since its inception. Prior to 1986, the Department mainly used contractors for overseas construction projects, and the total of contractors barely reached 50. Today, with the global war on terrorism and outsourcing initiatives being a dominant focus, the industrial security program is gaining momentum domestically and abroad, and the Department is increasing its dependence on contractor support.

While the Industrial Security Division is fully engaged with prospective contractors during the pre-award phase, after the contract is in place CORs and facility security officers frequently fail to notify the division when changes are made to a contract, such as when an employee is terminated.

(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)

(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)

(b) (2)(b) (2)(b) (2)(b) (2) . Other weaknesses in the program are inadequate controls over contracts not requiring access to classified or SBU material and the lack of a unified database of contractor information.

*Changes in Contract Employee Status*

Contractors frequently fail to notify the COR and/or the Industrial Security Division when an employee leaves or is removed from the contract. (b) (2)

<sup>6</sup> The National Industrial Security Program (NISP) was established by E.O. 12829.

(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)  
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)  
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)  
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)  
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)  
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)  
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)  
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)  
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)  
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)  
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)  
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)  
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)  
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)  
(b) (2)(b) (2)(b) (2)(b) (2)

Although there are procedures for revoking or modifying a contractor’s access to Department facilities based on his status within the contract, the Department is solely dependent on notification by the facility security officers or COR to set those procedures in motion. In addition, the process is fragmented, with no single office having access to all the elements to properly conduct oversight, including performing periodic audits. In addition, there is no automated electronic means to ensure this takes place. CORs and facility security officers need a better understanding of the importance of their reporting responsibilities, as required under 6 FAH-2 H-565 and 12 FAM 577.3.

**Recommendation 9:** The Foreign Service Institute should update the contracting officer’s representative training curriculum to emphasize the mandatory reporting of contract employee changes and the importance of retrieving badges when personnel are removed from a contract, as required by 6 FAH-2 H-565. (Action: FSI)

<sup>7</sup> Homeland Security Presidential Directive/HSPD-12, dates August 27, 2004; *Policy for a Common Identification Standard for Federal Employees and Contractors*.



**Recommendation 12:** The Bureau of Diplomatic Security should rewrite 12 FAM 570 to include review by the Industrial Security Division of those procurement packages that necessitate the issuance of a building pass to Department facilities or access to its information systems. (Action: DS, in coordination with A/OPE)

### *Information Databases*

The industrial security program is also hampered by the Industrial Security Division's inability to access common information and produce basic management reports. Tools and processes are inadequate for a program that is growing as much as the industrial security program. The division uses over five databases and programs to verify or obtain information on clearances, contract status, or badge information. Managers and team leaders do not have the management reporting tools they need to manage the program efficiently. Reports and simple management statistics cannot be easily generated, take days to generate, and, when produced, are either unreliable or incorrect. Managers and team leaders need, but do not have, access to databases that allows them to view current information and minimize repetitive data input. For example, a central repository for contractual information relating to Department contracts does not exist. The Industrial Security Division uses and maintains multiple databases and systems. Additionally, duplicative data entry results in inaccuracies and inefficiency, and is an error-prone process. Data (i.e., contract numbers, company names) is manually copied from one system to another. When OIG requested a report listing the firms that currently have connection to OpenNet, the division took three days to produce a response, which contained incorrect information. Two firms in the report had not done business with the Department in over a year. OIG informally recommended that a database be created to address the deficiencies cited above.

### *Management*

Overall, this division fosters a positive work environment in which employees are aware of customer service values. Having the division headed by strong leadership also promotes a proactive stance towards fulfilling its mission. The Industrial Security Division deserves credit for initiating the top-to-bottom review team and the OpenNet and ClassNet review team in its effort to ensure that information entrusted to private industry is appropriately safeguarded and protected. Both teams are new initiatives and are an example of the division chief's proactive management style.

External customers viewed guidance received by the division very positively, specifically in customer service, procedural guidance, staff expertise, and training. Within the industrial security program community, OIG believes there is a strong framework for information sharing and assistance to industry. However, Industrial Security Division employees do not believe that they are receiving adequate information from industry facility security officers or CORs regarding contract employee changes.

OIG found only one repeated concern by employees. This was regarding the unavailability of the division chief. Many of the 29 employees report having had less than two meetings with the division chief over the past year. With the recent creation of DS/SI and the many changes that have taken place within DS/SI and DS/SI/IS, regular, direct communication with division employees is essential. Both contractor and FTE employees voiced great respect for the division chief, feel their work is important, and believe they have received adequate training and the necessary tools to perform their job.

IND's staff growth has kept pace with its increased workload. The office has grown over five times its 1990's staffing level of five to its current level of 29 (11 FTE, 18 contractors). Much of this growth resulted from the Department's initiative on outsourcing, addressing serious security deficiencies discovered over the years, and implementing recommendations from the interagency top-to-bottom review team. The office appears to be rightsized for its current workload.

### *Program Applications Division*

The Program Applications Division, which has overall responsibility for managing the protection of the Department's classified and SBU information, has undertaken very positive initiatives in its security incident and open storage programs; however, improvements are needed in the Top Secret control officer and unit security officer programs.

The Program Applications Division is responsible for developing, defining, inspecting, and advising on facilities, procedures, and controls for safeguarding classified and administratively controlled information and for enforcing all associated security regulations. Division staff inspect facilities and train those employees requiring access to classified information, impressing upon them their individual responsibility for exercising vigilance and complying with the regulations for protecting classified and SBU material. Division staff continually review the implementation of these regulations to ensure that national security information is being properly safeguarded.

The Program Applications Division is responsible for many diverse programs relating to the protection of classified and SBU material: the security incident program, which includes damage assessments; domestic videoconferencing; TSCO program; unit security officers (USOs) and principal unit security officers (PUSOs) program, including conducting information security courtesy inspections; training for all employees with a security clearance, including Marine security guards and uniformed protective officers; and, certification of areas to be used as domestic strong rooms for the open storage of classified material.

Among all the programs the Program Applications Division is responsible for, it has made the most significant improvements in the security incident program. The division has begun providing Assistant Secretaries with semiannual reports of the numbers of security incidents, to bring greater management attentions to those offices and posts that need to improve. As a result of the division's concerted effort, the time required to investigate and adjudicate security incidents has steadily decreased, with the majority now taking less than thirty days.

#### *Management*

The Program Applications Division seems to be rightsized to accomplish its mission. However, overall management has suffered because of a long-standing vacancy in the division chief position. This position has been vacant for many years, having been filled by a series of temporary or acting division directors. This vacancy has adversely affected the management and morale of the division and has placed an added management burden on the office director, who must provide additional needed oversight, which takes time away from the overall management of the Office of Information Systems.

**Recommendation 13:** The Bureau of Diplomatic Security should fill the division chief position of the Applications Program Division in the Office of Information Security on a permanent basis. (Action: DS)

#### *Security Incident Program*

OIG found the security incident program to be well managed. The purpose of the program is to enhance the protection of classified information by identifying, evaluating, and assigning responsibility for breaches of security. A security incident is a failure to safeguard classified material in accordance with the governing regulations. The Program Applications Division adjudicates incidents to determine



Department's information security program, and therefore must take a more proactive role in ensuring bureaus compliance with the Top Secret control program.

12 FAM 535.1-2 b, states that domestically, the executive director of each bureau or major organizational element will designate, in writing, a bureau TSCO and an alternate to exercise control and maintain accountability records of material classified Top Secret in the custody of the bureau. The designated bureau TSCO will be a senior grade officer of the bureau who can control the dissemination and storage of the material. The bureau executive director is required to send a copy of the TSCO designation to the Program Applications Division. TSCOs are responsible for ensuring that Top Secret material is properly safeguarded, to include origination, marking, accountability, storage, duplication, transmission, and destruction per 12 FAM 512.1-6. The TSCOs are required to complete annual inventories by October 31 and submit a report to DS/ISP/APD. (b) (2)  
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)  
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)

**Recommendation 15:** The Bureau of Diplomatic Security should ensure that each Department bureau complies with Department requirements for the Top Secret control officer program. (Action: DS)

#### *Unit Security Officer Program*

The Program Applications Division does not have accurate records of assigned USOs and PUSOs and has not been responsive to the recommendations of a prior OIG review of the USO program.

12 FAM 563.1 requires domestically that the head of each major functional area designate a PUSO to assist in carrying out that area's security responsibilities. A PUSO is a managerial-level Department employee who is designated, in writing, by the bureau executive director to administer the security program in that organization and to maintain liaison with the Program Applications Division. PUSO designations must be forwarded to the division. PUSOs may designate and direct assistants (USOs), and written notification of these designations are required to be sent to the division. Any changes of PUSOs or USOs must also be reported to the Program Applications Division. According to 12 FAM 512.1-7, USOs have the supervisory and/or oversight responsibility to ensure that classified material entrusted to their organizational unit is handled in accordance with applicable procedures.



~~**SENSITIVE BUT UNCLASSIFIED**~~

~~**SENSITIVE BUT UNCLASSIFIED**~~

## MANAGEMENT CONTROLS

### CONTRACTING

DS/SI uses the support services of 236 contractor employees in its operations. It also uses the services of 619 special investigators hired under blanket purchase agreements to conduct background investigations. The total contract costs are over \$40 million annually. The ratio of contractors to direct hires, excluding blanket purchase agreements is almost two to one. In a contractor-intensive environment such as this, greater emphasis needs to be placed on contract administration.

#### *Acquisition Planning*

Requiring offices are responsible for ensuring that program requirements are clearly defined and the contract is designed to fulfill them. Requiring offices define the requirement, suggest sources for solicitation, prepare technical evaluation plans and criteria, and develop price estimates. In some instances, requiring offices have not properly performed their responsibilities and duties in accordance with FAR 7 - Acquisition Planning.

Specifically, requiring offices have not always submitted acquisition plans for major procurements. Department acquisitions regulations state that domestic requiring offices must develop a formal, written acquisition plan for all acquisitions exceeding \$5 million. Requiring offices should submit their acquisition plans to the appropriate contracting and procurement office.

**Recommendation 18:** The Bureau of Diplomatic Security should establish and implement procedures to ensure that all requiring offices develop and submit to the contract and procurement office a formal acquisition plan for all acquisitions exceeding \$5 million. (Action: DS)

Requiring offices do not submit technical requirements for some major acquisitions to contracting and procurement offices with sufficient lead-time necessary to promote full and open competition. In some instances, requirements were issued

on an urgent basis giving the contracting and procurement office less than four months to complete the acquisition process. In other instances, requiring offices have not submitted their requirements for follow-on contracts to active contracts that will expire in less than one year. There are legitimate reasons for issuing requirements urgently, but this practice should not be recurring as found in some acquisitions. Issuing requirements without sufficient lead-time restricts competition and increases prices. It also places a strain on the contracting and administrative staff. FAR 7.104 states that acquisition planning should begin as soon as the agency need is identified, preferably well in advance of the fiscal year in which contract award or order placement is necessary. OIG found little evidence that acquisition planning is being conducted within time frames suggested in FAR 7.104.

**Recommendation 19:** The Bureau of Diplomatic Security should issue a policy with guidelines that state minimum time frames needed to procure supplies and services with full and open competition. After establishing this policy, the Bureau of Diplomatic Security should monitor and track the performance of requiring offices to determine whether requiring offices are adhering to established policy. (Action: DS)

#### *Client Representative Training*

Client representatives are responsible for coordinating all matters related to DS task and delivery orders placed against contracts awarded by other agencies. Although client representatives have an important role in the administration of contracts, training for employees assigned to this function is insufficient. Client representatives do not receive formal training; only verbal instruction is given. There are also no standard operating procedures in place to guide employees serving in the role. This is a weakness in the procurement process, since client representatives are often coordinating tasks for multimillion-dollar orders for services that are crucial to operations. Interagency acquisition agreements state that the awarding agency's contracting officer is responsible for program oversight and managing day-to-day operations, but in practice it is the client representative who is handling these functions. In some cases, contracting officers are administering contracts out of field offices located thousands of miles away, thereby contracting officers place greater reliance on technical skills and managing capabilities of client representatives.



(b) (5)(b) (5)(b) (5)(b) (5)(b) (5)(b) (5)(b) (5)(b) (5)(b) (5)  
(b) (5)(b) (5)(b) (5)(b) (5)(b) (5)(b) (5)(b) (5)(b) (5)(b) (5)  
(b) (5)(b) (5)(b) (5)(b) (5)(b) (5)(b) (5)(b) (5)(b) (5)(b) (5)  
(b) (5)(b) (5)(b) (5)(b) (5)(b) (5)(b) (5)(b) (5)(b) (5)(b) (5)  
(b) (5)(b) (5)(b) (5)(b) (5)

In cases where the legal status of the contract is unclear, the contracting officer is responsible for making a decision as to whether proposed services are personal or nonpersonal services contracts. In this case the contracting officer's responsibility has not been exercised, per FAR 37.103(a).

In 2002, the Department gained statutory authority to hire personal services contractors, which would have allowed DS to convert blanket purchase agreements to personal services contracts and to hire additional personnel security specialists using this authority if needed. Instead of using this authority to hire additional personnel security specialists and resolve the legal issue, DS chose to use its contracting authority to hire 18 less experienced, higher priced personnel security specialists. If all option years are exercised on this contract, it will cost DS an estimated \$4 million above the cost to hire personal services contractors or direct-hire employees to perform the same work.

**Recommendation 21:** The Bureau of Diplomatic Security, in coordination with the Bureau of Administration and the Office of the Legal Adviser, should research and make a final determination as to whether personnel security specialists hired on blanket purchase agreements are considered personal services contracts or nonpersonal service contracts. (Action: DS, in coordination with A/LM and L)

*Contract Files*

During the course of this inspection, OIG observed that some official correspondence and documents were missing from contract files. In addition, the Office of the Legal Adviser was unable to produce some official correspondence related to the use of blanket purchase agreements. There should be greater emphasis on recordkeeping.

*Memorandum of Understanding*

A memorandum of understanding for security support services is needed between DS and OPM. DS conducts overseas background investigations for OPM, and in exchange OPM conducts national agency check on Department nonsensitive positions and gives DS access to OPM's databases. Under the Omnibus Diplomatic Security Act (P.L. 99-399), DS may provide services to U.S. government departments and agencies through the establishment of memoranda of understanding on security support abroad. The Department has signed agreements with several agencies, but there is no existing agreement for this arrangement with OPM. DS also provides security support services for the FBI, but there is no memorandum of understanding outlining the agreement between DS and the FBI.

DS's current arrangements with these agencies are for an exchange of services; no cost or charge for service is involved. The Economy Act authorizes an agency to enter into agreements with other agencies for goods and services and requires each ordering agency to reimburse the performing agency for the actual cost of services provided. Memoranda of understanding should be entered into under the provisions of the Economy Act (31 U.S.C 1535 and 1536).

**Recommendation 22:** The Bureau of Diplomatic Security should complete and sign a memorandum of understanding for security support services provided for the Office of Personnel Management. The memorandum of understanding should be entered into under the provisions of the Economy Act (31 U.S.C 1535 and 1536). (Action: DS)

**Recommendation 23:** The Bureau of Diplomatic Security should complete and sign a memorandum of understanding for security support services provided for the Federal Bureau of Investigation. The memorandum of understanding should be entered into under the provisions of the Economy Act (31 U.S.C 1535 and 1536). (Action: DS)

## INTERNAL SECURITY

Although, as discussed above, improvements are needed in the administration of the unit security officer program, overall the internal security of the three offices of DS/SI is adequate and appropriate. Classified material is being properly stored



## INFORMATION RESOURCE MANAGEMENT

OIG found that DS's chief technology officer provides the necessary information management support to DS/SI. However, the existence on the DS/SI system of inappropriate material and unauthorized software shows a need for additional attention. Also, the chief technology officer's information system security officer (ISSO) does not have the access to the systems he needs to perform his duties.

The chief technology officer has developed standard operating procedures for the bureau's information systems. The bureau has established a local information technology configuration control board and has provided computer security awareness training to its users. Bureau information technology staff has developed information system security program plans and contingency plans for the DS/SI major applications, including the Baseline Tool Kit and the Computer Incident Response Tracking Database. The ISSO regularly reviews system logs for abnormal activity and follows up on computer incidents. The ISSO also sends computer security reminder e-mails to users.

### *Inappropriate Files*

OIG found inappropriate material including sexual cartoons and pictures on the DS/SI information systems. 5 FAM 723 prohibits sexually explicit material on government computer systems. Upon finding inappropriate material, the ISSO warns the user to remove the inappropriate material and she follows up three days after she sends the warning notice. If the inappropriate material is not removed, she then sends system access revocation warnings to the user. The user's supervisor is also notified of the inappropriate use of government information systems. Such actions are appropriate. The ISSO stated that her staff provides weekly activity reports on the specific domains that were reviewed. However, the inappropriate material found shows that information security management controls, including monitoring of user libraries and mailboxes, need to be improved.

**Recommendation 25:** The Bureau of Diplomatic Security should implement a more strategic monitoring schedule to scan all Directorate of Security Infrastructure servers and network resources for inappropriate material. (Action: DS)

*Unauthorized Software*

OIG also found unauthorized software such as games, contact databases, and electronic facsimile applications installed on DS/SI information systems. 12 FAM 625.1 explicitly prohibits the installation of unapproved software on Department information systems. Upon finding the unauthorized software, the ISSO warns the user to remove the software and then follows up after the warning notice is sent. If the software is not removed, a system access revocation warning is sent to the user. The user's supervisor is also notified of the installation of the unauthorized software and the possible revocation of system access. The installation of unapproved software could lead to the introduction of potential malicious code into the DS information systems.

**Recommendation 26:** The Bureau of Diplomatic Security should implement a monitoring schedule to ensure that only Department-approved software is installed on government computers. (Action: DS)

*Information Systems Security Officer Access*

OIG found that the bureau's ISSO does not have the authority to perform the oversight duties, as required by the 12 FAM 600 series, on DS/SI/CS's SBU information systems domain because she lacks systems access to the DS/SI/CS domain. She stated that the DS/SI/CS domain is separate from the DS domain. It is imperative that the bureau's ISSO have access to all bureau information systems to perform oversight. (b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2) (b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)

**Recommendation 27:** The Bureau of Diplomatic Security should ensure that the information systems security officer has access to all domains in order to perform oversight duties. (Action: DS)



**Recommendation 8:** The Bureau of Diplomatic Security should, in coordination with the Bureau of Administration and the Bureau of Intelligence and Research, develop and implement a plan to relocate all personnel of the Special Security Operations Division, Office of Information Security, into the Harry S Truman building and to provide additional office space for the division's document control and operations support branches. (Action: DS, in coordination with A/OPR and INR)

**Recommendation 9:** The Foreign Service Institute should update the contracting officer's representative training curriculum to emphasize the mandatory reporting of contract employee changes and the importance of retrieving badges when personnel are removed from a contract, as required by 6 FAH-2 H-565. (Action: FSI)

**Recommendation 10:** The Bureau of Administration, Office of the Procurement Executive, should issue a procurement information bulletin emphasizing the need for contracting officer's representatives to report contract employee changes and the importance of retrieving badges when personnel are removed from a contract. (Action: A/OPE)

**Recommendation 11:** The Bureau of Administration, Office of the Procurement Executive, should include a clause in all contracts requiring notification to the Bureau of Diplomatic Security when a cleared contract employee terminates and the immediate return of the employee's Department badge. (Action: A/OPE)

**Recommendation 12:** The Bureau of Diplomatic Security should rewrite 12 FAM 570 to include review by the Industrial Security Division of those procurement packages that necessitate the issuance of a building pass to Department facilities or access to its information systems. (Action: DS, in coordination with A/OPE)

**Recommendation 13:** The Bureau of Diplomatic Security should fill the division chief position of the Applications Program Division in the Office of Information Security on a permanent basis. (Action: DS)

**Recommendation 14:** The Bureau of Diplomatic Security should take necessary steps to ensure that regional security officers submit the Notice of Security Incident (OF-117) and Record of Incident (OF-118) in a timely manner, including revising 12 FAM 553 to specify a required time frame for their submission. (Action: DS)

- Recommendation 15:** The Bureau of Diplomatic Security should ensure that each Department bureau complies with Department requirements for the Top Secret control officer program. (Action: DS)
- Recommendation 16:** The Bureau of Diplomatic Security should ensure that each Department bureau complies with Department requirements for the unit security officer program. (Action: DS)
- Recommendation 17:** The Bureau of Diplomatic Security should respond as required to the Office of Inspector General report *Follow-up Review of the Unit Security Officer Program*, SIO/C-03-35. (Action: DS)
- Recommendation 18:** The Bureau of Diplomatic Security should establish and implement procedures to ensure that all requiring offices develop and submit to the contract and procurement office a formal acquisition plan for all acquisitions exceeding \$5 million. (Action: DS)
- Recommendation 19:** The Bureau of Diplomatic Security should issue a policy with guidelines that state minimum time frames needed to procure supplies and services with full and open competition. After establishing this policy, the Bureau of Diplomatic Security should monitor and track the performance of requiring offices to determine whether requiring offices are adhering to established policy. (Action: DS)
- Recommendation 20:** The Bureau of Diplomatic Security, in coordination with the Foreign Service Institute, should develop a training program specifically designed to train client representatives. (Action: DS, in coordination with FSI)
- Recommendation 21:** The Bureau of Diplomatic Security, in coordination with the Bureau of Administration, Office of Acquisitions, and the Office of the Legal Adviser, should research and make a final determination as to whether personnel security specialists hired on blanket purchase agreements are considered personal services contracts or nonpersonal service contracts. (Action: DS, in coordination with A/LM/AQM and L)
- Recommendation 22:** The Bureau of Diplomatic Security should complete and sign a memorandum of understanding for security support services provided for the Office of Personnel Management. The memorandum of understanding should be entered into under the provisions of the Economy Act (31 U.S.C 1535 and 1536). (Action: DS)

**Recommendation 23:** The Bureau of Diplomatic Security should complete and sign a memorandum of understanding for security support services provided for the Federal Bureau of Investigations. The memorandum of understanding should be entered into under the provisions of the Economy Act (31 U.S.C 1535 and 1536). (Action: DS)

**Recommendation 24:** (b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)  
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)  
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)

**Recommendation 25:** The Bureau of Diplomatic Security should implement a more strategic monitoring schedule to scan all Directorate of Security Infrastructure servers and network resources for inappropriate material. (Action: DS)

**Recommendation 26:** The Bureau of Diplomatic Security should implement a monitoring schedule to ensure that only Department-approved software is installed on government computers. (Action: DS)

**Recommendation 27:** The Bureau of Diplomatic Security should ensure that the information systems security officer has access to all domains in order to perform oversight duties. (Action: DS)

## INFORMAL RECOMMENDATIONS

Informal recommendations cover operational matters not requiring action by organizations outside the inspected unit and/or the parent regional bureau. Informal recommendations will not be subject to the OIG compliance process. However, any subsequent OIG inspection or onsite compliance review will assess the mission's progress in implementing the informal recommendations.

### *Office of Personnel Security and Suitability*

OIG and the results of the risk assessment questionnaire identified a need for improved and continual training in the investigative and adjudicative functions.

**Informal Recommendation 1:** The Office of Personnel Security and Suitability, with the assistance of the Bureau of Diplomatic Security's Office of Training and Performance Support, should develop a staff training plan for continuing education.

The office's size, intense workload, and vulnerability to lapses in internal management controls raise questions regarding the effective span of control of the office director.

**Informal Recommendation 2:** The Bureau of Diplomatic Security should review the Office of Personnel Security and Suitability's organizational structure and supervisory span of control to determine if a deputy director position is warranted.

Adverse action cases are not entered into DS/SI/PSS databases such as RMS and CMS due to privacy considerations. Status and management reports must be compiled from Microsoft Word files, largely denying the Adverse Actions Division the benefits of automation. While the number of pending cases is not large, the numbers mount up over time. Automation would enhance both accountability and productivity. It may be possible to define an adverse action role in RMS that would allow only Adverse Actions Division staff to access adverse action cases.

**Informal Recommendation 3:** The Bureau of Diplomatic Security chief technology officer should study the possibility of integrating adverse action cases into the Report Management System database. A memo reporting the conclusions of the study should be sent to the coordinator of the Directorate of Security Infrastructure.

Employees in DS/SI/PSS do not have a clear understanding of the purpose of the proposed reorganization of the adjudications function.

**Informal Recommendation 4:** The Bureau of Diplomatic Security should hold regular all-hands staff meetings to keep employees informed of the reorganization process.

### *Management Controls*

In some instances, official correspondence and documents were missing from contract files.

**Informal Recommendation 5:** The Bureau of Diplomatic Security, in coordination with the Bureau of Administration's Office of Acquisitions should establish, maintain, and dispose of contract files in accordance with regulations contained in FAR 4.8 - *Government Contract Files*.

In some instances, databases that contain contract and logistical information are not always accurate.

**Informal Recommendation 6:** The Bureau of Diplomatic Security should periodically review and update databases to ensure that contract and logistical information is accurate.

Requiring offices do not always provide the DS Contracts and Procurement Branch with timely information needed to update databases containing contract and logistical information.

**Informal Recommendation 7:** The Bureau of Diplomatic Security should issue an administrative notice reminding requiring offices of the importance of keeping databases accurate.

*Information Resource Management*

Security container check sheets, SF-702, are not being posted to every repository containing classified material, as required by 12 FAM 539.1.

**Informal Recommendation 8:** The Bureau of Diplomatic Security should ensure that a security container check sheet, SF-702, is posted to every repository containing classified material.

~~**SENSITIVE BUT UNCLASSIFIED**~~

~~**SENSITIVE BUT UNCLASSIFIED**~~

## PRINCIPAL OFFICIALS

Senior Coordinator for the Directorate of  
Security Infrastructure

Donald Reid

Office Directors:

Office of Personnel Security and Suitability  
Office of Computer Security  
Office of Information Security

James Onusko  
Mary Stone Holland  
Cheryl Hess

~~**SENSITIVE BUT UNCLASSIFIED**~~

~~**SENSITIVE BUT UNCLASSIFIED**~~

## ABBREVIATIONS

|            |  |
|------------|--|
| CMS        | Case Management System                                       |
| COR        | Contracting officer's representative                         |
| DCID       | Director of Central Intelligence Directive                   |
| Department | Department of State  |
| DISCO      | Defense Industrial Security Clearance Office                 |
| DS         | Bureau of Diplomatic Security                                |
| DSS        | Bureau of Diplomatic Security's Diplomatic Security Service  |
| DS/SI      | Directorate of Security Infrastructure                       |
| DS/SI/CS   | Office of Computer Security                                  |
| DS/SI/IS   | Office of Information Security                               |
| DS/SI/PSS  | Office of Personnel Security and Suitability                 |
| e-QIP      | OPM's electronic questionnaire for investigations processing |
| FBI        | Federal Bureau of Investigation                              |
| FTE        | Full-time equivalent   |
| HST        | Harry S Truman building                                      |
| ICC        | Interim clearance coordinator                                |
| ISSO       | Information systems security officer                         |
| OIG        | Office of Inspector General                                  |
| OPM        | Office of Personnel Management                               |
| PSC        | Personal services contract                                   |
| PUSO       | Principal unit security officer                              |
| RCSO       | Regional computer security officer                           |
| RMS        | Report Management System                                     |

|      |  |
|------|--|
| RSO  | Regional security officer  |
| SBU  | Sensitive But Unclassified   |
| SCI  | Sensitive Compartmented Information  |
| SCIF | Sensitive compartmented information facility                               |
| SIO  | Office of Inspector General, Office of Security and Intelligence Oversight |
| TSCO | Top Secret control officer   |
| USO  | Unit security officer  |

## APPENDIX I - PRIOR AUDITS AND INSPECTIONS

Following is a list of recent OIG audits and compliance follow-up reviews of specific programs and activities that are under the responsibility of the Bureau of Diplomatic Security's Directorate of Security Infrastructure.

- Management of Sensitive Compartment Information Access, SIO/A-98-49 (SBU/NOFORN)*
- Protecting Classified Documents at State Department Headquarters, SIO/A-99-46 (SBU)*
- Audit of the Department's Background Investigations, 01-SIO-R-061 (Unclassified)*
- Enhancing the Protection of Classified Material at State Department Headquarters, SIO/A-02-35 (SBU)*
- Protection of Classified Documents at State Department Headquarters, SIO/A-03-30 (SBU)*
- Follow-up Review of the Unit Security Officer Program, SIO/C-03-35 (SBU)*
- Protection of Classified Information at State Department Headquarters, SIO/A-04-11 (Secret)*
- Protection of SCI at Department Headquarters, (Currently in draft; report to be issued in FY 2005)*

**FRAUD, WASTE, ABUSE, OR MISMANAGEMENT**  
of Federal programs  
and resources hurts everyone.

Call the Office of Inspector General  
**HOTLINE**  
**202-647-3320**  
**or 1-800-409-9926**  
**or e-mail [oighotline@state.gov](mailto:oighotline@state.gov)**  
to report illegal or wasteful activities.

You may also write to  
Office of Inspector General  
U.S. Department of State  
Post Office Box 9778  
Arlington, VA 22219  
Please visit our Web site at:  
<http://oig.state.gov>

Cables to the Inspector General  
should be slugged "OIG Channel"  
to ensure confidentiality.