OIG
Office of Inspector General
U.S. Department of State • Broadcasting Board of Governors

ISP-I-16-28A | Office of Inspections | September 2016

Inspection of the Bureau of Diplomatic Security, Threat Investigations and Analysis Directorate

DOMESTIC OPERATIONS

OIG HIGHLIGHTS

September 2016
OFFICE OF INSPECTIONS
Domestic Operations

Inspection of the Bureau of Diplomatic Security, Threat Investigations and Analysis Directorate

ISP-I-16-28A

What OIG Inspected

OIG inspected the Bureau of Diplomatic Security, Threat Investigations and Analysis Directorate, from February 5 to March 7, 2016.

What OIG Recommended

OIG made five recommendations to the Bureau of Diplomatic Security to improve operations and internal control in the Threat Investigations and Analysis Directorate.

What OIG Found

- The Threat Investigations and Analysis Directorate was accomplishing its stated mission "to protect life safety."
- The Directorate's decision to shift to a proactive approach to threat management expanded its mission and workload without a commensurate increase in human resources.
- Coordination and communication were effective at senior levels of the Threat Investigations and Analysis Directorate, but senior managers did not communicate consistently with mid-level staff members, adversely affecting the Directorate's ability to efficiently meet its defined objectives and goals.

Office of Inspector General
U.S. Department of State • Broadcasting Board of Governors

CONTENTS

CONTEXT

"To protect life safety" is the stated mission of the Bureau of Diplomatic Security, Threat Investigations and Analysis Directorate (Directorate). The Directorate's four offices are the Bureau of Diplomatic Security's (DS) primary means of gathering, analyzing, investigating, and disseminating threat information to protect American interests worldwide. The Directorate reports threats directly to the Assistant Secretary for Diplomatic Security, among others, and to Regional Security Officers (RSO) at overseas posts. It also supplies threat analyses to assistant secretaries of regional bureaus as well as to private-sector constituents. In addition, the Directorate assigns country-specific threat levels, in consultation with posts and regional bureaus, in the annual Security Environment Threat List. A Deputy Assistant Secretary (DAS) oversees the Directorate and reports through the Principal Deputy Assistant Secretary to the DS Assistant Secretary.

DS created the Directorate in 2008 by combining four existing offices. Each office is led and managed by an office director and has its own defined role in handling, analyzing, or investigating threat information:

- The Office of Intelligence and Threat Analysis (ITA) analyzes all-source intelligence on terrorist activities and threats directed against chief of mission personnel and U.S. diplomatic facilities overseas. The office also monitors threats against the Secretary of State, U.S. Government officials, foreign dignitaries visiting the United States, and U.S.-based foreign diplomats and missions. ITA previously had been part of the DS International Programs Directorate.

- The Diplomatic Security Command Center (DSCC) provides 24-hour law enforcement and security command and control operations for incidents worldwide that have a nexus to U.S. Government interests and specific DS global missions. DSCC also functions as the DS focal point for receiving and disseminating information, especially during a crisis, and serves as the DS liaison with other U.S. Government watch centers. Prior to being incorporated into the Directorate, DSCC was a stand-alone office reporting directly to the DS Front Office. This is the first time that OIG has inspected the DSCC.

- The Overseas Security Advisory Council (OSAC) promotes security cooperation between the Department and U.S. private-sector interests (businesses, non-governmental organizations, educational institutions, and faith-based groups). It provides private entities with regular and timely information on overseas security developments by establishing Country Councils at U.S. missions overseas and Regional Councils and Sector Specific Working Groups domestically. It also provides guidance to the private sector in coordinating security planning and implementing security programs. OSAC is a public-private partnership with a constituent base of 12,653 users representing 3,934 private-sector entities (as of September 30, 2015). Subject matter experts from U.S. Government agencies serve as technical advisors to OSAC. Prior to the Directorate's formation, OSAC reported directly to the DS Front Office. This is the first time OIG has inspected OSAC.

- The Office of Protective Intelligence Investigations (PII) directs, coordinates, and conducts investigations and implements threat management plans related to terrorism and other threats—including potential threats—against the Secretary of State; U.S. Government employees, facilities, and interests under chief of mission authority overseas; Department personnel and facilities; and foreign mission personnel and facilities. PII has representatives in the National Counterterrorism Center, the Joint Interagency Task Force, and 26 regional Federal Bureau of Investigation/Interagency Joint Terrorism Task Forces (JTTF). PII also includes the Department's counterterrorism program Rewards for Justice. Although the Directorate assumed responsibility for PII from the DS Domestic Operations Directorate in 2008, it assumed oversight for JTTF in 2011 This is the first time that IG has inspected PII.

Appendix C provides examples to illustrate the roles of the Directorate's different offices. The Directorate organizational chart is in Appendix D.

The Classified Annex to this report discusses security issues related to the Directorate.

EXECUTIVE DIRECTION

OIG based the following assessments of Directorate leadership on the results of 64 documented interviews that elicited comments on the Front Office, 166 surveys completed by Directorate staff members, and OIG's review of documents and observations of meetings and activities during the course of the on-site inspection.

Execution of Foreign Policy Goals and Objectives

Directorate's Strategic Approach to Threat Management: Proactive

The Directorate's objective is to develop intelligence information to prepare for and mitigate threats rather than simply react to crises. This change in approach from reactive to proactive is an initiative promoted from within the Directorate and is largely the work of the DAS and office directors, all of whom were nearing the end of their tours when the inspection began. This proactive approach had translated into new initiatives, such as ITA's threat analyst program, PII's expanded support for the Secretary's protective detail, and DSCC's now-regular support to joint operations command centers at special events. The DS Assistant Secretary expressed support for these initiatives. The OSAC expansion of services and products for its private-sector constituents had been ongoing. The Directorate's leadership set priorities and established programs through discussions between the DAS and the office directors who met with employees to gather input for these discussions. Additionally, the DS Assistant Secretary and Principal Deputy Assistant Secretary provided direction to the Directorate and met regularly with the DAS.

Despite Staffing Challenges and Expanding Responsibilities, the Directorate Accomplished its Mission

Despite taking on new responsibilities without additional staff and facing a high turnover among existing personnel, the Directorate achieved its mission. It had, however, requested additional staff to alleviate the burden on its employees. ITA told OIG that since 2010, its taskings had increased by approximately 300 percent; PII stated its mission to provide more proactive security had increased the agent workload "exponentially;" DSCC stated that watch officer responsibilities had steadily increased, especially in the post-Benghazi period. Despite these challenges, the Directorate asserted—and OIG agreed, based on input from the Directorate's customers and OIG's review of its products—that it remained effective in achieving its core life safety objectives.

The Directorate requested additional staff in January 2016, when Directorate leadership told the Assistant Secretary that in the absence of increased staff, it was "in danger of not meeting our basic responsibility to analyze, assess, investigate and disseminate threat information and the myriad of other duties for which we are responsible." This theme was repeated in memoranda prepared for OIG and in personal interviews OIG conducted throughout the Directorate.

The DS Assistant Secretary told OIG that decisions about additional personnel would have to wait until the release of a bureau-wide staffing study, expected in August 2016, that he had ordered. That study, he said, would provide metrics to determine where DS should allocate its personnel.

Management Challenges: Coordination and Communication

OIG found that increased staffing alone would be insufficient to address the Directorate's management challenges. For example, a lack of coordination and communication between its offices and officers was unrelated to staffing shortfalls. OIG learned that mid-level officers were unfamiliar with the work of other Directorate offices; they did not have a clear understanding of how their work related to that of the Directorate overall; and they did not understand how their functions complemented those of similarly situated staff in other Directorate offices. This lack of familiarity created a risk that staff members would miss opportunities to work more efficiently. Moreover, it was sometimes difficult for them to prioritize tasks and define their audiences in an organization where everything related to the broad mission of protecting life safety. Mid-level staff members also cited the need for greater top-down and lateral communication. Principle 14.02 of the Government Accountability Office *Standards for Internal Control in the Federal Government*[1] emphasizes that management should communicate quality information throughout an entity using established reporting lines and to communicate down, across, up, and around reporting lines to all levels of the entity.

[1] General Accountability Office, *Standards for Internal Control in the Federal Government* (GAO-14-704G, September 2014), Principle 14.01.

OIG discussed these concerns with Directorate leadership and suggested that they improve communication by holding more frequent town hall and staff meetings. OIG also advised leadership to consider how it allocated scarce personnel resources to eliminate redundancies and less-essential tasks to free more time for core responsibilities. To address immediate staffing gaps, OIG suggested that the Directorate consider a range of short-term solutions, particularly while the bureau was engaged in its long-term staffing alignment initiative, using the Strategic Workforce Alignment and Planning tool to help make management decisions on where and how resources should be invested.

Tone at the Top

The Directorate's DAS retired on March 4, 2016, days before the end of this inspection. The DS front office chose the ITA office director to replace him. OIG did not evaluate how the new DAS set the tone at the top—leading by example and demonstrating the organization's values, philosophy, and operating style—because he started the position at the close of the inspection. However, OIG expressed the concern that his direct and forceful communication style, as demonstrated during his tenure as ITA office director, risked inhibiting the free flow of communication in a directorate that was, as discussed above, already challenged by communications issues. OIG advised the new DAS of the importance of adhering to the Leadership and Management Principles for Department Employees outlined in 3 Foreign Affairs Manual (FAM) 1214 b(4). These address the need for leaders to express themselves clearly and effectively, offer and solicit constructive feedback from others, and anticipate varying points of view by soliciting input.

Internal Control

Top Managers Not Held Accountable for Internal Control Assurance Process

The Directorate's DAS and office directors did not provide annual internal control assurance statements for the Department's annual Management Control Assurance Process[2]. Although lower-level Directorate staff completed the survey questionnaires DS used to confirm compliance with internal control requirements, Directorate managers did not complete assurance statements—as required in 2 FAM 024 of all office directors and higher level officials—due to lack of understanding of the requirements. As a result, DS had no documentation showing that Directorate leaders confirmed adherence to internal control requirements.

The Department's FY 2015 annual Management Control Assurance Process memorandum advised that, "Just as the Secretary's statement will rely on your assurance statement, your assurance statement must be supported by input from your managers reporting to you." The DS

[2] The Department's Management Control Assurance Process is conducted pursuant to the Federal Managers Financial Integrity Act of 1982. It requires that the Secretary provide an annual statement to the President and Congress commenting on the adequacy of the Department's systems of management control.

Executive Director stated in an August 2015 memorandum that "Each Division Chief, Officer Director, or DAS must complete the survey for their immediate office."

The FAM and these memoranda make clear management's responsibility for determining the adequacy of internal controls in their organizations. Absent Directorate leadership statements, there is a risk that the Directorate's internal control practices will fall short of requirements; deficiencies and weaknesses may not be identified; Directorate management may not know what staff reported in surveys; and DS management may not take appropriate corrective actions..

Recommendation 1: The Bureau of Diplomatic Security should require the Threat Investigations and Analysis Directorate to implement a policy to provide annual Management Control Assurance Process statements. (Action: DS)

POLICY AND PROGRAM IMPLEMENTATION

Office of Intelligence and Threat Analysis

ITA is comprised of four divisions. Three of these consist of seven geographic teams that handle and analyze threat information related to their specific regions of the world and contribute to the Security Environment Threat List. The Directorate created a fourth division—Logistics, Liaison, Training, and Production—in 2015 to provide administrative support.

Customers for ITA's products told OIG the office provided information that is useful and relevant and that it was achieving its defined objectives.

Lack of Top-down Communication

ITA management had not communicated mission-critical information to the staff. For example, during the inspection OIG found that ITA analysts were unaware of leadership's decision on membership in the U.S. Government Intelligence Community. Of the 23 ITA analysts interviewed, half cited advantages of membership, including the increased access to information and training that they believed it would bring. ITA leadership, however, told OIG that it had already concluded that it was more advantageous for ITA to not join the Intelligence Community but had not informed the staff of its decision.

In addition, analysts were unclear about the audience for the threat assessments they prepared. Some told OIG their audience was RSOs overseas while others believed they wrote for the DS Assistant Secretary. Assessments written for agents in the field included more detailed information while assessments for the DS senior leaders included a higher level summary. The lack of clarity about the audience created a risk that analysts would not tailor their threat assessments appropriately.

The Government Accountability Office *Standards for Internal Control in the Federal Government* requires managers to internally communicate necessary information to achieve the entity's objectives. OIG advised ITA leadership to communicate its views on membership in the Intelligence Community to staff members and to clarify the audience for threat assessments.

Office Cannot Evaluate Its Products Without Customer Feedback

ITA had not implemented a regular process of soliciting feedback on the quality and focus of their assessments from its customers. ITA told OIG it was unaware of the need for its staff to receive regular feedback. ITA last sent surveys soliciting feedback in May 2009 and October 2015. Without regular customer feedback, analysts do now know if their threat assessments are useful and relevant. Regularly soliciting feedback would enable ITA to better assess whether it is meeting its mission and objectives. The Government Accountability Office *Standards for Internal Control in the Federal Government* emphasize the importance that communication from management and outside parties plays in helping organizations achieve their objectives and address related risks.[3]

Recommendation 2: The Bureau of Diplomatic Security should implement a policy to solicit customer feedback from recipients of Office of Intelligence and Threat Analysis threat assessments. (Action: DS)

Deployed Threat Analyst Program

New Program to Assign Intelligence Analysts to Embassies Proves Unworkable

At the time of the inspection, the Directorate was in the first year of the Deployed Threat Analyst Program, an ITA initiative that sought to place Foreign Service officers trained by ITA as intelligence analysts at embassies in countries designated as high risk for terrorism. Directorate leaders told OIG that after considering lessons learned in this first year, they concluded that the program was unworkable for a variety of practical and logistical reasons. Among them were the difficulty the Directorate faced recruiting employees with the requisite intelligence experience and challenges in arranging for appropriate secure embassy workspaces.

As a result of these and other unforeseen difficulties, Directorate leaders decided to discontinue the program in its current form.

Office of Protective Intelligence and Investigations

PII includes three divisions: the Operations and Investigations Division (OID), the Intelligence and Liaison Division (ILD), and the Rewards for Justice Program. PII works with investigations and intelligence, taking raw intelligence and turning it into an actionable threat management plan or investigation.

[3] GAO-14-704G, Principle 15.07.

On the basis of interviews with more than 20 PII customers from other agencies and within the Department, OIG concluded that PII customers were satisfied with the support they received.

ILD supports the bureau by coordinating DS operations and investigative efforts with the Intelligence Community, Department of Defense, the National Counter-Terrorism Center, the Federal Bureau of Investigation's Counter Terrorism division, and National JTTF. More broadly, ILD agents were assigned to 26 regional JTTFs, headed by the FBI but comprised of representatives of the law enforcement and intelligence communities. ILD agents were also assigned to JTTF extraterritorial units, whose mission was to deploy and investigate acts of international terrorism focused against U.S. interests.

Expanded Workload Strains Manpower

During the preceding 5 years, PII took on additional workload without increasing its staff. In the past, PII augmented the Secretary's security detail on specific overseas trips, assigning one or more special agents or intelligence analysts to provide intelligence and investigative expertise to the DS teams traveling with the Secretary. At the time of the inspection, PII supported the Secretary on all trips, including domestic travel. PII also expanded its support of DS coverage of special events, such as the World Cup. OIG reviewed the number of hours agents (but not intelligence analysts) devoted to these duties during 2015 and found this additional travel took agents away from the office for approximately 3,380 person-days. This equated to roughly one-third of PII's deployable agents, leaving the remaining agents to accomplish what a significantly larger staff had previously done. With fewer agents in the office, it became especially important that staff members prioritized the demands on their time.

Principle 5 of the Government Accountability Office *Standards for Internal Control in the Federal Government* requires managers to evaluate and adjust excessive pressure to help personnel fulfill their assigned responsibilities. Failing to adjust these pressures increases the risk of creating a culture of cutting corners and degradation in the quality of work. OIG advised PII leaders to assess its staffing needs and realign or adjust staffing to meet current priorities.

Operations and Investigations Division

Supervisors do Not Readily Know the Status of Investigative Cases

OID supervisors did not regularly meet with case officers to review the status of their work and as a result, often did not have accurate, up-to-date case information. OIG discussed with OID managers the importance of regular meetings between supervisors and investigators to review case status. This ensures that supervisors have accurate case information and maintain administrative control over investigations.

Taskings are Not Coordinated

OID used a management structure in which all employees shared responsibility for fulfilling the same range of tasks. This structure had advantages for fast-paced offices like OID where acting quickly was a priority in that it gave managers the flexibility to place employees where needed

as demands changed. Another consequence, however, was that functional supervisors in OID were unaware of the current workload for each employee. Under OID's organizational structure, any supervisor can assign a task to any of the division analysts or investigators. Directly tasking the employee, without clearing it with the employee's functional supervisor, can lead to conflicting assignments and imbalanced workloads. OIG advised OID managers to adopt work practices that ensure that functional supervisors fully understand their subordinates' range of assignments. Such a step would allow supervisors to take corrective action to ensure workload balance.

Diplomatic Security Command Center

According to its website, DSCC "is the eyes and ears of the organization, a 24/7 watch office that provides real-time information to decision makers as events unfold." The center uses a range of sophisticated technologies to monitor the security of overseas facilities and personnel in real time. In times of crisis, DSCC provides the command and control function to support all aspects of the DS response.

DSCC relays all-source threat information to RSOs and passes security incident information received from RSOs to DS in Washington, to other Department offices, and to other agencies. At the time of the inspection, the DSCC Technical Operations Group was monitoring and responding to Intrusion Detection and Imminent Danger Notification activations from 299 facilities worldwide. The Technical Operations Group maintained the ability to monitor security cameras at all posts worldwide. DSCC had the ability to track the location of U.S. Government personnel traveling or conducting operations in hostile/hazardous areas via its Personnel Tracking Locator system.

No Metrics for Gauging Customer Satisfaction

DSCC customers in the Department and other agencies told OIG that they judged DSCC's information to be unique and useful. DSCC did not, however, systematically solicit input from its customers and had no metric for measuring customer satisfaction. OIG advised DSCC to implement a policy of periodic surveys or other suitable methods to gauge customer satisfaction. Such feedback would enable DSCC to confirm whether it is giving customers what they need and would help DSCC refine its products.

Overuse of the Law Enforcement Sensitive Caveat Limits Dissemination of Information

Customers told OIG that DSCC information was sometimes incomplete because the office had not passed on information that was labeled Law Enforcement Sensitive (LES). This information typically is unclassified and not subject to release under Freedom of Information Act exemption 7 of 5 U.S. Code 552 because such release could put an investigation or an individual at risk. DS policy prohibits passing LES information to non-law enforcement authorities without a need to know. DSCC personnel interviewed by OIG could not provide a clear explanation for when the LES designation would be used. DSCC management had not provided clear guidance to DSCC watch personnel on handling information marked LES and the redaction process so that the information could be expeditiously forwarded to its customers. Additionally, DS had not

provided clear guidance to RSOs on when to use the LES caveat on the information it sends to DSCC.

Recommendation 3: The Bureau of Diplomatic Security should provide clear guidance for use of the Law Enforcement Sensitive designation and create a standard operating procedure for reviewing and redacting information designated Law Enforcement Sensitive. (Action: DS)

Overseas Security Advisory Council

From interviews with more than 20 OSAC private-sector constituents and U.S. Government technical advisors, OIG concluded that the council met its customers' needs. Customers consistently told OIG they considered OSAC's mission to be important and that they highly valued its products. OSAC solicited constituent input through multiple formal and informal mechanisms and used customer feedback to refine its products.

The Research and Information Support Center is the heart of the OSAC analysis operation. It consisted of three functional units: Research and Analysis, Outreach and Engagement, and Global Security. These units had day-to-day contact with their private-sector constituents and exchanged security information through phone consultations, frequent meetings, and myriad products published on the OSAC website. This website was OSAC's primary means of communicating with private-sector constituents and U.S. Government associates. In the fourth quarter of FY 2015, the website received 440,070 visits, a 17-percent increase over the same quarter in FY 2014. In February 2016, OSAC launched mobile apps to give users instant access to website reports and allow them to more easily submit incident reports from remote locations.

Short-term Extensions for Third Party Contractor Employees Create Challenges

Twenty-one of the 35 positions in OSAC are third-party contractor employees working in the Research and Information Support Center, which provides analytical support to constituents. That labor contract, managed by the Bureau of Administration, expired in September 2013. Since then, the Bureau of Administration continued the current contract through a series of short-term extensions and bridge contracts while soliciting a new contract under a HubZone set-aside[4].

This extended period without a long-term contract, and the uncertainty associated with last-minute temporary renewals, created challenges for OSAC and adversely affected its ability to undertake long-term planning for travel and other critical mission needs. On occasion, the office could only purchase costly one-way plane tickets rather than less expensive round trip tickets, and at times staff faced the possibility of becoming stranded overseas. In addition, the contract

[4] The Small Business Administration's HUBZone program is in line with the efforts of both the Administration and Congress to promote economic development and employment growth in distressed areas by providing access to more federal contracting opportunities.

re-competition process required extensive and on-going participation by the Research and Information Support Center chief, to the detriment of his other regular mission-critical duties. The Bureau of Administration acknowledged that the contract status created challenges for OSAC, but told OIG they were unavoidable given the Department's procurement priorities and the legal requirements concerning the new contract solicitation.

Another problem, over which the Directorate had no control but which its leadership told OIG affected all offices, was the length of time it took for new hires to receive security clearances. At the time of inspection, 60 percent of the positions in the Research and Information Support Center's Global Security Unit were vacant because the employees hired to fill them had yet to receive security clearances. This adversely affected that division's ability to disseminate information to private-sector constituents. OSAC had extended employment offers to replacement personnel, but prolonged delays in obtaining the required security clearances prevented them from reporting for duty.

RESOURCE MANAGEMENT

Staff Resources

Mandatory Training Is Not Tracked or Enforced

The Directorate did not uniformly track employee compliance with mandatory training requirements due to inadequate attention by management. Tracking is necessary to enforce the Department-mandated training requirements—including training in leadership and supervision, Equal Employment Opportunity principles, and ethics—required by 13 FAM 300. As a result, management did not know whether staff had completed mandatory training. The Directorate improved its management of training in other ways, including establishing standard operating procedures for training. But without knowing whether staff had completed mandatory training, the Directorate could not conduct workforce planning effectively. Additionally, without assurance that employees received this training, supervisors did not know whether their employees had the skills and knowledge taught in the mandatory courses.

According to 13 FAM 022.4, bureau training officers are responsible for identifying employee training needs and reporting on training activities. DS training officers were not performing this function. However, 13 FAM 022.5 also states that managers and supervisors are responsible for (1) Determining the specific needs of their employees and ensuring that employees receive training for effective job performance; and (2) Ensuring that they and their employees have current and up-to-date training.

Recommendation 4: The Bureau of Diplomatic Security should implement a mechanism to track and enforce mandatory training for employees of the Threat Investigations and Analysis Directorate. (Action: DS)

Reviewing Officers for ILD JTTF Agents Not Directly Involved in Those Activities

PII assigned special agents to the 26 regional JTTFs around the United States. The reviewing officers for those agents' annual Foreign Service Employee Evaluation Reports were officers at the DS field offices with responsibility for the JTTF geographic locations. However, these reviewing officers did not have access to the JTTF agents' work product or familiarity with their daily activities. DS field office reviewers also were not in a position to regularly observe the interactions between the DS JTTF agents and their ILD rating officers. According to 3 Foreign Affairs Handbook-1 H2813.1c, "reviewing officers should acquaint themselves with employees whose ratings they review and develop personal knowledge of their performance." This reviewing arrangement began when the Directorate assumed oversight for JTTF in April 2011. Having officers who are unfamiliar with the work of the special agents responsible for reviewing their performance creates a risk that the evaluations will be inaccurate. OIG advised DS to consider realigning reviewing responsibilities for special agents assigned to JTTFs and designate reviewing officers who are familiar with the special agents' work.

Information Management

Uncoordinated Requests for IT Support Contribute to Delays

Directorate employees rated the level of IT support below average on OIG questionnaires. The Directorate received information management and information security support from two providers. The Bureau of Information Resource Management (IRM) provided desktop support while the DS Office of the Chief Technology Officer provided support for bureau-specific applications and for those desktop functions not covered by IRM.

OIG found that resolution times for trouble tickets were within performance metrics outlined in the IRM service level agreement. From January 1 through February 19, 2016, the Directorate reported 320 trouble tickets, all of which were assigned to IRM for resolution. The issues included resetting user accounts, installing applications, and basic network connectivity matters. The IRM service level agreement for consolidated bureaus requires resolution for trouble tickets within 30 minutes for critical issues to a maximum of 48 hours for low-priority issues. Of the 320 reported tickets, IRM resolved 278 (87 percent) within the required time.

Among the reasons IT technicians cited for longer resolution times—up to 9 days for the remaining 13 percent of the tickets—were unclear descriptions of issues and the inability of the technician to contact the affected user. OIG advised Directorate management to consider assigning a single point of contact in each office to coordinate IT service requests.

New Analysts Wait for Access to Classified Networks

Lengthy delays in new employees receiving classified network accounts contributed to staffing challenges in the Directorate. Employees reported waiting from a few weeks to several months after beginning work before they received their accounts and could begin performing their jobs. Access to the classified network is critical for Directorate analysts, who use the network to review

and send cables and intelligence information. Approval from several DS offices and the Bureau of Intelligence and Research was required for new classified accounts. In September 2015, Directorate staff met with relevant parties to identify delays and improve information flow and the clearance process. As a result, DS developed a standard operating procedure that tracked the status of requests and helped speed up the process. The Directorate reported that a recent new employee, using this procedure, received a classified account within 1 week. The Directorate expressed hope that this would become the norm for receiving new accounts

Websites Contain Outdated Information

Some Directorate websites contained outdated information. As a result, viewers could have received inaccurate, incomplete, or irrelevant information. The Directorate had not established an organization-wide policy for regularly updating webpage content. With the exception of OSAC, which updated its website regularly, Directorate office managers had not emphasized the need to maintain website content, nor had they ensured that staff were allocated time to do so. According to 5 FAM 776.2b, content managers are required to ensure that information published on websites is current, relevant, and accurate.

Recommendation 5: The Bureau of Diplomatic Security should establish a policy to regularly update content on all Threat Investigations and Analysis Directorate websites. (Action: DS)

RECOMMENDATIONS

Recommendation 1: The Bureau of Diplomatic Security should require the Threat Investigations and Analysis Directorate to implement a policy to provide annual Management Control Assurance Process statements. (Action: DS)

Recommendation 2: The Bureau of Diplomatic Security should implement a policy to solicit customer feedback from recipients of Office of Intelligence and Threat Analysis threat assessments. (Action: DS)

Recommendation 3: The Bureau of Diplomatic Security should provide clear guidance for use of the Law Enforcement Sensitive designation and create a standard operating procedure for reviewing and redacting information designated Law Enforcement Sensitive. (Action: DS)

Recommendation 4: The Bureau of Diplomatic Security should implement a mechanism to track and enforce mandatory training for employees of the Threat Investigations and Analysis Directorate. (Action: DS)

Recommendation 5: The Bureau of Diplomatic Security should establish a policy to regularly update content on all Threat Investigations and Analysis Directorate websites. (Action: DS)

PRINCIPAL OFFICIALS

Title	Name	Arrival Date
Front Office:		
Acting Deputy Assistant Secretary	Kurt Rice	6/2011
Office Directors:		
Office Director, PII	Carlos Matus	10/2011
Executive Director, OSAC	Stephen P. Brunette	6/2014
Executive Director, ITA	Kurt Rice	6/2011
Office Director, DSCC	Todd Ziccarelli	3/2013

Source: Threat Investigations and Analysis Directorate

APPENDIX A: PURPOSE, SCOPE, AND METHODOLOGY

This inspection was conducted in accordance with the Quality Standards for Inspection and Evaluation, as issued in 2012 by the Council of the Inspectors General on Integrity and Efficiency, and the Inspector's Handbook, as issued by OIG for the Department of State and the Broadcasting Board of Governors.

Purpose and Scope

The Office of Inspections provides the Secretary of State, the Chairman of the Broadcasting Board of Governors, and Congress with systematic and independent evaluations of the operations of the Department and the Broadcasting Board of Governors. Inspections cover three broad areas, consistent with Section 209 of the Foreign Service Act of 1980:

- **Policy Implementation:** whether policy goals and objectives are being effectively achieved; whether U.S. interests are being accurately and effectively represented; and whether all elements of an office or mission are being adequately coordinated.
- **Resource Management:** whether resources are being used and managed with maximum efficiency, effectiveness, and economy and whether financial transactions and accounts are properly conducted, maintained, and reported.
- **Management Controls:** whether the administration of activities and operations meets the requirements of applicable laws and regulations; whether internal management controls have been instituted to ensure quality of performance and reduce the likelihood of mismanagement; whether instance of fraud, waste, or abuse exist; and whether adequate steps for detection, correction, and prevention have been taken.

Methodology

In conducting inspections, OIG reviews pertinent records; as appropriate, circulates, reviews, and compiles the results of survey instruments; conducts onsite interviews; and reviews the substance of the report and its findings and recommendations with offices, individuals, organizations, and activities affected by the review.

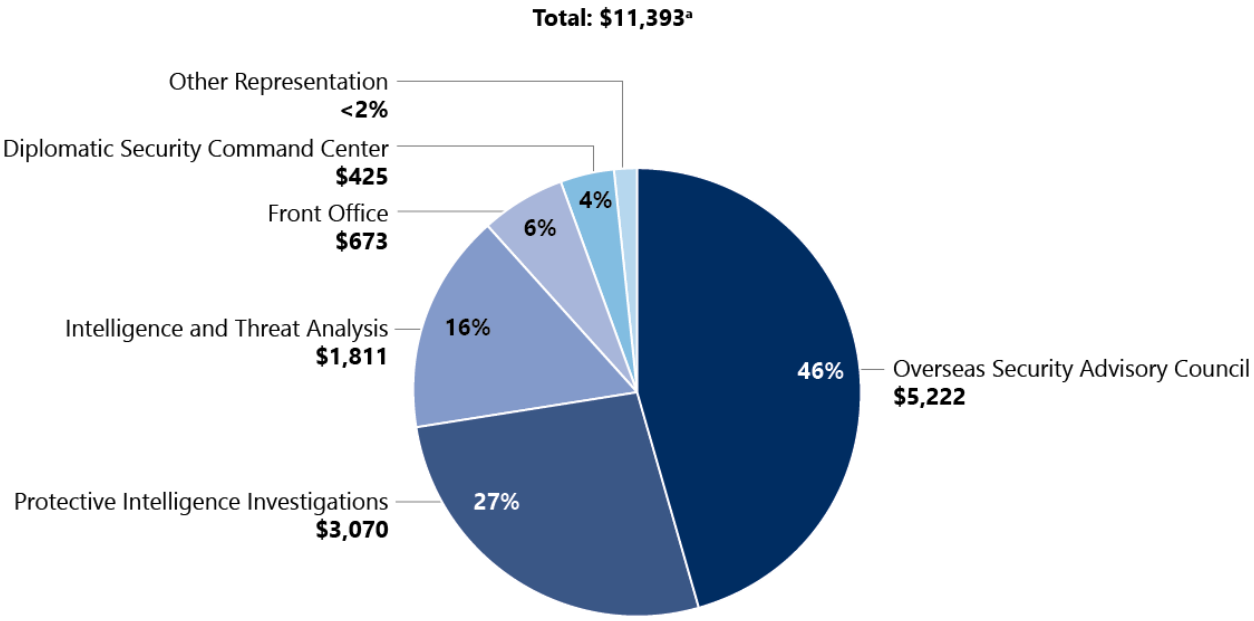
For this inspection, OIG conducted 186 documented interviews and reviewed 323 surveys or documents.

APPENDIX B: FY 2015 STAFFING AND BUREAU-MANAGED FUNDING

Financial Resources

Figure 1: Bureau of Diplomatic Security, Directorate of Threat Investigations and Analysis, FY 2015 Program Budget

($ Thousands)

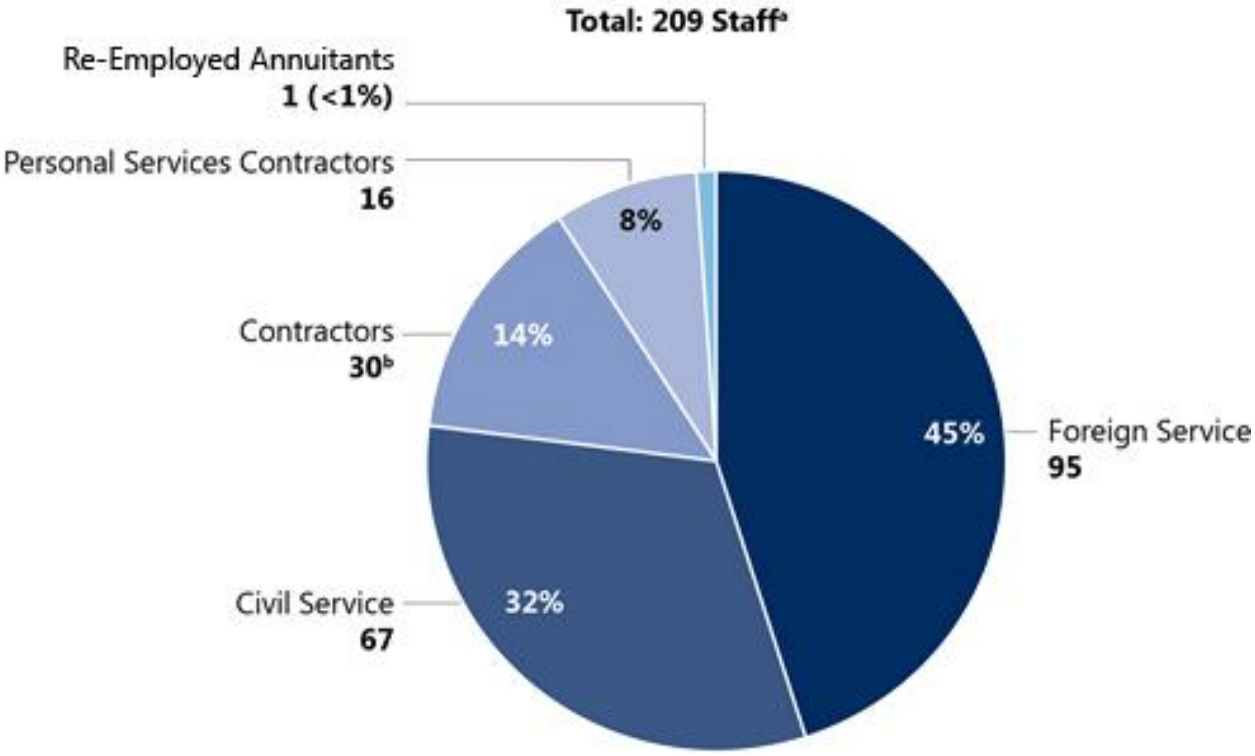


[a] In FY 2015, the Directorate managed $11.4 million in the Worldwide Security Protection Account (Diplomatic and Consular Program funds). This excluded funding for salaries for Full Time Equivalent personnel, which were funded separately through a centrally managed account. It also did not include Rewards for Justice payments made in FY 2015 from the K fund. It did include costs for personnel working as personal service contractors and for third-party contractor personnel.

Source: Bureau of Diplomatic Security, Office of Executive Director, Comptroller.

Human Resources

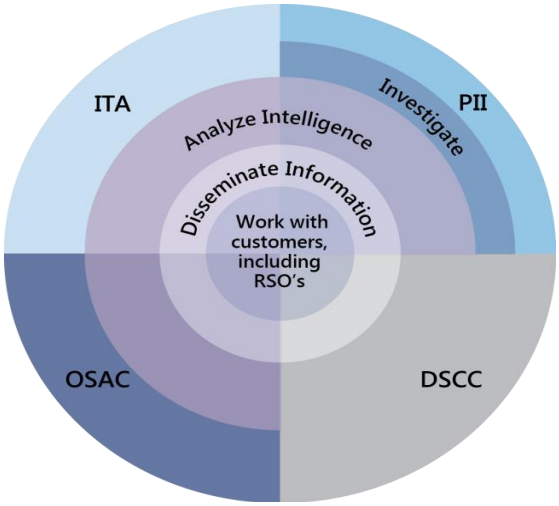
Figure 2: Bureau of Diplomatic Security, Directorate of Threat Investigations and Analysis



[a] Does not include staff members from outside agencies detailed to the Directorate. Rounding creates a total of less than 100 percent.
[b] Does not include 19 DS Office of Security Technology contract staff members on duty in DSCC.

Source: Bureau of Diplomatic Security, Office of Executive Director, as of March 4, 2016.

APPENDIX C: EXAMPLES OF DIRECTORATE OFFICE COMPLEMENTARY ROLES



Source: OIG created these hypothetical examples based on information learned during the inspection. They are provided for illustrative purposes.

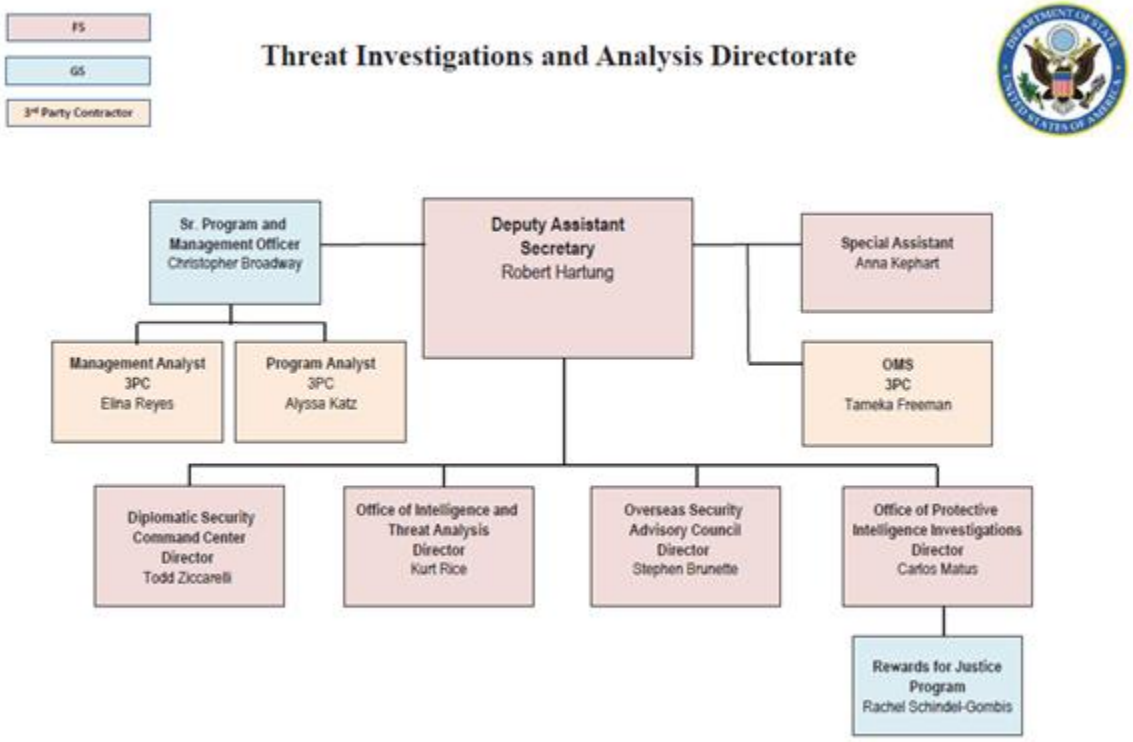
ITA Example: ITA advises an Ambassador and his RSO that a terrorist cell in their country has begun coordinating with Islamic State of Iraq and the Levant operatives in a neighboring country. The information may be cautionary or may indicate imminent operational activity. Information about a plan of terrorist action against U.S. interests or citizens may or may not be specific but is adequate to assist post in planning mitigation. These threats are simultaneously conveyed to all DS directorates (by DSCC) so DS can marshal the personnel and material required to mitigate threats large and small.

PII Example: After an Ambassador's motorcade is attacked, PII quickly deploys to work closely with the RSO, host country authorities, and other law enforcement agencies to lead the investigation for DS. PII investigates leads, conducts interviews, collects evidence, and manages the investigation for DS in preparation for possible prosecution. Using investigative techniques and all-source intelligence, PII works to identify who conducted the attack, how it was conducted, and possible motives behind the attack to assist DS in responding to the incident and mitigating future threats.

DSCC Example: During a crisis, DSCC takes calls from the RSO at the embassy affected. It passes that information on to other DS offices and other Department and interagency interlocutors, and it relays information to the embassy. During non-crisis times, DSCC monitors embassy security measures (door alarms, surveillance cameras, personnel locators) in real time. It takes incoming calls from RSOs and relays information to them; conducts law enforcement records checks supporting the DS criminal programs, and relays incident information received from posts to ITA and PII as well as to DS and other Department leadership as appropriate.

OSAC Example: OSAC learns of a specific threat of a terrorist plan to attack a named off-shore oil platform of a U.S. company. OSAC obtains cleared language from the originator of the report and sends threat information to the embassy RSO in that country, who contacts the company in country and provides security guidance. OSAC also passes the threat information to the company's headquarters in the United States. Outside of direct threat passage, OSAC analysts write reports on security issues facing the private sector, answer questions from constituents, and conduct outreach to the private sector through consultations and Country Council meetings.

APPENDIX D: DIRECTORATE ORGANIZATIONAL CHART



ABBREVIATIONS

DAS	Deputy Assistant Secretary
Directorate	Threat Investigations and Analysis Directorate
DS	Bureau of Diplomatic Security
DSCC	Diplomatic Security Command Center
FAM	Foreign Affairs Manual
ILD	Intelligence and Liaison Division
IRM	Bureau of Information Resource Management
ITA	Office of Intelligence and Threat Analysis
JTTF	Joint Terrorism Task Force
LES	Law Enforcement Sensitive
OID	Operations and Investigations Division
OSAC	Overseas Security Advisory Council
PII	Office of Protective Intelligence Investigations
RSO	Regional Security Officer

OIG INSPECTION TEAM MEMBERS

Lisa Bobbie Schreiber Hughes, Team Leader
Paul Cantrell, Deputy Team Leader
Ronald Deutch
Gary Herbst
Leo Hession
Vandana Patel
Richard Sypher

HELP FIGHT

FRAUD. WASTE. ABUSE.

1-800-409-9926
OIG.state.gov/HOTLINE
If you fear reprisal, contact the
OIG Whistleblower Ombudsman to learn more about your rights:
OIGWPEAOmbuds@state.gov