Inspector General Statement on the Department of State's Major Management and Performance Challenges

FISCAL YEAR
2017

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

OIG-EX-18-02

CONTENTS

CONTENTS 1
INTRODUCTION 1
PROTECTION OF PEOPLE AND FACILITIES 3
Constructing and Maintaining Safe and Secure Diplomatic Facilities 3
Ensuring the Health and Safety of Personnel Abroad 4
Operations of Official Vehicles Overseas 5
Residential Security 6
Emergency Preparedness 7
OVERSIGHT OF CONTRACTS, GRANTS, AND FOREIGN ASSISTANCE 8
Managing Grants in Compliance With Applicable Standards 8
Ensuring Proper Invoice Review and Approval Processes 9
Monitoring and Documenting Contractor Performance 10
INFORMATION SECURITY AND MANAGEMENT 12
Strengthening Cybersecurity Practices 12
Establishing Effective Records Management Programs 15
FINANCIAL AND PROPERTY MANAGEMENT 15
Identifying Internal Control Deficiencies 16
Complying With Internal Controls 17
Tracking and Reporting Department Assets 18
Collecting, Analyzing, and Using Financial Information 19
Seeking Reimbursement and Sharing Costs for Services Provided 20
OPERATING IN CONTINGENCY AND CRITICAL ENVIRONMENTS 21
WORKFORCE MANAGEMENT 23
PROMOTING ACCOUNTABILITY THROUGH INTERNAL COORDINATION AND CLEAR LINES OF AUTHORITY 25
CONCLUSION 27
APPENDIX A: RESPONSE FROM THE DEPARTMENT OF STATE 29

INTRODUCTION

Each year, as required by law,[1] the Office of Inspector General (OIG) for the Department of State (Department) identifies the most serious management and performance challenges facing the Department and briefly assesses the Department's progress in addressing those challenges. The resulting report is included in the Department's annual agency financial report.

Based on our oversight work performed this year and in the past, research, and independent judgment, OIG concludes that the following are the major management and performance challenges the Department faced in FY 2017:

- Protection of people and facilities
- Oversight of contracts, grants, and foreign assistance
- Information security and management
- Financial and property management
- Operating in contingency and critical environments
- Workforce management
- Promoting accountability through internal coordination and clear lines of authority

Each of these challenges affects the Department's ability to achieve its substantive mission. In this report, we identify situations in which our oversight work found that the Department has addressed these concerns, but we focus primarily on the work that led us to include the challenge in the first place. We also identify some of OIG's specific recommendations associated with these issues.

Three of these challenges—protection of people and facilities; oversight of contracts, grants, and foreign assistance; and information security and management—are largely unchanged from our FY 2016 management challenges report and from our reports on this topic from the past several years. These issues go to the heart of the Department's programs and operations, and it is likely that these will be crucial challenges for the foreseeable future. Nonetheless, the specific ways that these challenges manifest themselves change over time, and our work in FY 2017 focused on particular aspects of these problems.

Two challenges that we identified in past reports—financial management and managing posts and programs in conflict zones—have been modified. In preceding years, we identified financial management as a key challenge for the Department, and this is still an area where the Department can improve. This year, however, we broaden the challenge to include a wider range of financial

[1] The Reports Consolidation Act of 2000, § 3, Pub. L. 106-531 (amending 31 U.S.C. § 3516).

issues as well as property management. Our analysis of this issue particularly considers the effect of certain internal control deficiencies—specifically, management failure to identify deficiencies and poor adherence to established internal control processes—on the Department's ability to safeguard its financial resources and property. Additionally, we address weaknesses in tracking and reporting data, analyzing and using financial data effectively, and effectively seeking reimbursement for services and implementing cost-sharing measures. We also broaden our discussion of the unique challenges the Department faces operating in zones experiencing contingency operations. We reframe this challenge to address contingency zones and otherwise critical environments. Our reports have found that many of the same types of logistical and security concerns arise in locations that are recovering from disasters (including disease) or civil strife but are not actively involved in conflicts.

Finally, this year we have added two new challenges: workforce management and promoting accountability through coordination and clear lines of authority. We include workforce management because OIG's reports have identified difficulties associated with lack of, or poor use of, personnel resources, such as inadequate training and overly short rotations. We address issues of coordination and authority because OIG has identified these concerns in a wide range of programs. Without clearly defined roles and responsibilities and effective coordination among Department entities with intersecting obligations, the Department's ability to effectively carry out its programs and operations is compromised.

These challenges are not necessarily found in isolation. Rather, they tend to compound each other. To take just one example, contract oversight in conflict zones, where Department employees frequently have short rotations and limited ability to monitor performance, presents a situation where management challenges related to oversight of contracts, operating in critical environments, and workforce management overlap. Other problems, such as weaknesses in IT security, are exacerbated in situations where there are unclear or overlapping lines of authorities.

Continued attention to the management challenges identified in this report will improve the Department's operations and, accordingly, its ability to fulfill its mission and to be a good steward of taxpayer resources. OIG particularly encourages the Department to consider ways that specific recommendations might be applied broadly to make more systemic changes that will improve the Department's overall operations and to ensure that these changes contribute to meaningful, permanent changes in practice. We hope that this report, read together with the work OIG produces throughout the year, assists the Department in its efforts.

PROTECTION OF PEOPLE AND FACILITIES

The protection of its people and facilities abroad remains a serious management and performance challenge for the Department. The threat of physical violence against U.S. diplomats and U.S. diplomatic facilities touches every region of the world. In its most recent compilation of incidents of political violence against Americans abroad, the Bureau of Diplomatic Security (DS) described numerous incidents that involved diplomats and diplomatic facilities as targets. These included, for example, incidents in which armed men fired at a vehicle carrying embassy personnel in Haiti, an individual threw a brick at Consulate General Hong Kong, and a knife-wielding assailant attacked a guard stationed outside of Embassy Nairobi in Kenya.[2] The threat of physical violence is naturally greater in conflict areas, such as Iraq and Afghanistan, that are at the forefront of U.S. engagement to defeat terrorism. Nonetheless, attacks in Belgium, France, Turkey, and elsewhere underscore the global nature of these threats. Additionally, natural disasters, environmental hazards, and ordinary crime continually pose risks to the health and safety of Department personnel and their families serving abroad. Much of OIG's work identifies risks to Department personnel and facilities and provides recommendations to address those risks.

Constructing and Maintaining Safe and Secure Diplomatic Facilities

The Department places great emphasis on the need to provide safe and secure facilities abroad. It expends significant resources on maintaining, updating, and expanding its more than 270 diplomatic missions abroad—some of them large, sprawling compounds.

Nonetheless, OIG found physical security deficiencies at U.S. diplomatic missions covered in its FY 2017 reports. Many of the reports related to this issue are classified, but publicly available information illustrates the challenges the Department faces in this area. For example, in one of two reports relating to Embassy Kabul in Afghanistan, OIG found that, after installation and inspection by DS, two security doors at the embassy were improperly altered, which potentially affected their overall security performance.[3] In a separate report on the construction of two buildings at Embassy Kabul, OIG found that poor quality assurance and oversight of the construction process led to myriad instances of

[2] Department of State Bureau of Diplomatic Security, *Political Violence Against Americans 2016* (May 2017).

[3] OIG, *Management Assistance Report: Improvements Needed to the Security Certification Process To Ensure Compliance With Security Standards at Embassy Kabul, Afghanistan* (AUD-MERO-17-28, March 2017).

failure to adhere to electrical and fire safety standards.[4] Throughout FY 2017, OIG inspections of U.S. embassies identified numerous facility maintenance deficiencies, including partially collapsed and leaky roofs, and nonfunctioning fire alarms.[5]

Constructing and maintaining safe and secure diplomatic facilities is always a challenge, and that challenge is compounded in regions afflicted by conflict and humanitarian crises. For several years, OIG has, however, recommended various steps the Department could take to improve adherence to its own policies and processes. For example, the Bureau of Overseas Buildings Operations (OBO) and DS should develop and implement formal, standardized processes to prioritize physical security-related deficiencies at posts by category.[6] OBO should also implement an effective process to respond to posts' formal requests for physical security-related funding.[7] Additionally, the Department should modify the security certification process to include a follow-up inspection by DS that would prevent alterations such as those identified at Embassy Kabul from going unnoticed.[8] Finally, overseas posts should follow the Department's facilities maintenance policies, including implementing required comprehensive preventive, routine, and special maintenance programs. OIG has, for the most part, made recommendations directed toward the practices of particular posts but encourages the Department to consider whether similar concerns at other locations could be addressed as well.

Ensuring the Health and Safety of Personnel Abroad

The Department pays serious attention to the security, and more generally, the overall health and safety of its personnel abroad. OIG reviewed its findings on executive direction from the past 3 years of inspection reports and concluded that, in more than 70 percent of the reports, embassy leadership was engaged on security issues and supported the Regional Security Officer and other

---

[4] OIG, *Management Assistance Report: Building Deficiencies Identified at U.S. Embassy Kabul, Afghanistan Need Prompt Attention* (AUD-MERO-17-44, June 2017).

[5] OIG, *Inspection of Embassy Monrovia, Liberia* (ISP-I-17-12, May 2017); OIG, *Inspection of Embassy Freetown, Sierra Leone* (ISP-I-17-16, May 2017).

[6] OIG, *Management Assistance Report: Department Attention Needed to Address Overdue Responses on Selected Open Recommendations* (AUD-ACF-17-55, July 2017); OIG, *Compliance Follow-up Audit of the Process To Request and Prioritize Physical Security-Related Activities at Overseas Posts* (AUD-ACF-16-20, December 2015); OIG, *Audit of the Process To Request and Prioritize Physical Security-Related Activities at Overseas Posts* (AUD-FM-14-17, March 2014).

[7] *Ibid.*

[8] In particular, OIG recommended that OBO, in coordination with DS, revise the physical security certification process to include a follow-up inspection by DS to confirm that OBO took actions to address all identified deficiencies in accordance with physical security standards before occupancy. AUD-MERO-17-28, March 2017. OBO did not concur with this recommendation, and, as of September 30, 2017, OIG considers the recommendation unresolved.

mission elements that contributed to an effective security, health, and safety posture.[9] This is, however, an area that requires constant attention, and, throughout its FY 2017 reports, OIG identified specific areas in which the Department could do better. As described below, OIG noted continuing concerns with the operations of official vehicles overseas and certain aspects of residential security.

Operations of Official Vehicles Overseas

In several FY 2017 reports, OIG detailed deficiencies in the management and operation of official vehicles at overseas posts. For example, in an audit of the administration of the armored vehicle program, OIG found that some posts used armored vehicles that did not meet required protective standards; OIG also found that some posts did not have enough armored vehicles to provide an enhanced level of protection for their employees.[10] Furthermore, OIG identified problems with the maintenance of armored vehicles, including inadequate tire pressure and extensive damage to windshields.[11] These deficiencies can directly affect the safety and utility of these vehicles.

Compounding those problems are deficiencies in driver training, an issue that OIG has previously identified.[12] For example, OIG found that most chauffeurs at Mission Pakistan lacked armored vehicle training even though the mission's own travel policy mandates the use of armored vehicles for all vehicle movements.[13] OIG also reported instances where inadequate driver training extended beyond armored vehicle operators. In particular, several inspection reports discussed posts that did not ensure that all their chauffeurs and incidental drivers received appropriate training.[14] Some posts also failed to ensure drivers had required medical certifications[15] and adhered to Department limits on working hours.[16] At Embassy Tel Aviv—a post with a high number of

---

[9] OIG, *Management Assistance Report: Department Can Take Steps Toward More Effective Executive Direction of Overseas Missions* (ISP-17-38, July 2017).

[10] OIG, *Audit of the Bureau of Diplomatic Security's Administration of the Armored Vehicle Program* (AUD-SI-17-21, February 2017).

[11] *Ibid.*

[12] OIG, *Management Assistance Report: Armored Vehicle Training* (ISP-16-17, July 2016).

[13] OIG, *Inspection of Embassy Islamabad, Pakistan* (ISP-I-17-11A, February 2017).

[14] OIG, *Inspection of Embassy Tel Aviv, Israel* (ISP-I-17-20, May 2017); OIG, *Inspection of Embassy Bishkek, Kyrgyzstan* (ISP-I-17-13, March 2017); ISP-I-17-12, May 2017; ISP-I-17-16, May 2017.

[15] ISP-I-17-20, May 2017; ISP-I-17-12, May 2017; ISP-I-17-16, May 2017.

[16] ISP-I-17-20, May 2017; ISP-I-17-16, May 2017.

preventable vehicle mishaps—OIG also found that the embassy did not impose disciplinary measures on three drivers with repeated motor vehicle mishaps.[17]

Some of these issues are limited to practices at particular posts. More generally, though, OIG recommendations have identified potential improvements in program management practices that could minimize these deficiencies. For example, the Department should develop and implement a detailed plan for the armored vehicle program and hire an experienced program manager to oversee the fleet. Regarding the acquisition and maintenance of armored vehicles, the Department should bolster its internal policies requiring adherence to its standards.[18] Furthermore, given that Department personnel posted abroad rely heavily on official vehicles, posts should ensure that supervisors are not disregarding limits on working hours, overlooking requirements for medical certifications and driving training, or ignoring appropriate occasions to administer disciplinary measures.

Residential Security

In FY 2017, OIG identified some posts that largely complied with the Department's standards for residential safety and security. For example, a limited-scope inspection of Embassy Kingston in Jamaica revealed a housing pool that generally met Department standards.[19] Additionally, OIG found that new employees received briefings that outlined the critical crime threat in Jamaica and policies and directives related to personnel security restrictions.[20]

In many other posts, however, OIG continued to find deficiencies in the administration of the Department's housing and related anti-crime program. Multiple inspections identified posts that had not ensured that residential properties met the Department's fire safety standards.[21] For example, in Luanda, Angola, OIG reported that 28 of the 38 government-leased apartments in a high-rise building did not meet fire safety requirements and concluded they should be removed from the housing pool.[22] Additionally, OIG identified several posts that had not properly inspected or could not demonstrate they had

---

[17] ISP-I-17-20, May 2017. OIG notes that, based on its recommendations to improve the motor vehicle safety management program and the Department's efforts, Embassy Tel Aviv has significantly decreased motor vehicle mishaps.

[18] AUD-SI-17-21, February 2017.

[19] OIG, *Inspection of Emergency Preparedness and Residential Security at Embassy Kingston, Jamaica* (ISP-I-17-25A, June 2017).

[20] *Ibid.*

[21] OIG, *Inspection of Embassy Belgrade, Serbia* (ISP-I-17-08A, January 2017); OIG, *Inspection of Embassy Luanda, Angola* (ISP-I-17-19, June 2017); ISP-I-17-12, May 2017.

[22] ISP-I-17-19, June 2017.

properly inspected residential properties for health and safety risks before assigning employees to occupy them.[23]

Extended staffing gaps, particularly in the position of Post Occupation Safety and Health Officer, underlie these deficiencies in some cases. Given the implications for the health and safety of Department personnel and their families, however, overseas posts should focus on complying with the Department's standards pertaining to residential properties, including completing and documenting required safety and health inspections and residential security surveys.

Emergency Preparedness

Department guidelines require U.S. embassies to maintain post-specific emergency action plans to respond to situations such as bombs, fires, civil disorders, and evacuations. Many FY 2017 inspections of overseas posts noted broad compliance with Department emergency planning standards and solid engagement on the issue from front office leadership. To take one example, Embassy Bishkek in Kyrgyzstan took intermediate and long-term steps to obtain a housing pool of seismically secure residences.[24]

OIG, however, continued to note deficiencies that present safety risks to Department personnel and American citizens abroad in the event of a natural disaster or other crisis. These included consular sections that did not comply with Department standards for emergency preparedness[25] and inadequate testing and maintenance of important hardware necessary for communication during a crisis, including satellite phones and high-frequency radios.[26] OIG also found that, despite being at a high risk for earthquakes, Embassy Rangoon in Burma had not conducted adequate earthquake drills or training and had no seismic surveys for any of the buildings in its residential housing pool.[27]

In some cases, staffing shortages and competing priorities were cited as factors in these deficiencies. Nonetheless, because of the importance of the issue, OIG has issued various recommendations that overseas posts should comply with the Department's emergency preparedness policies, including conducting required drills and ensuring consular staff are trained on their roles during a crisis.

---

[23] OIG, *Inspection of Bratislava, Slovakia* (ISP-I-17-06A, January 2017); OIG, *Inspection of Port Moresby, Papua New Guinea* (ISP-I-17-07A, January 2017); ISP-I-17-19, June 2017; ISP-I-17-20, May 2017; ISP-I-17-13, March 2017.

[24] ISP-I-17-13, March 2017.

[25] ISP-I-17-12, May 2017; ISP-I-17-16, May 2017.

[26] OIG, *Inspection of Emergency Preparedness at Consulate General Hamilton, Bermuda* (ISP-I-17-26, May 2017); ISP-I-17-25A, June 2017.

[27] OIG, *Inspection of Embassy Rangoon, Burma* (ISP-I-17-05A, January 2017).

OVERSIGHT OF CONTRACTS, GRANTS, AND FOREIGN ASSISTANCE

The Department spends substantial resources by means of contracts, grants, and cooperative agreements. In FY 2016 alone, the Department's obligations included more than $15 billion for contracted services and more than $18 billion in grants and fixed charges.[28] To meet its obligation to use taxpayer resources prudently, the Department must ensure that contractors and grantees are appropriately selected, work is properly conducted and monitored, objectives of the grant or contract are achieved, and costs are effectively contained. Oversight of these resources continues to be a significant management challenge for the Department. Inadequate oversight and mismanagement pose substantial financial risk to the Department. Moreover, oversight weaknesses and mismanagement also increase the possibility that the purpose of these instruments will not be met.

Managing Grants in Compliance With Applicable Standards

Throughout the year, various reports identified posts and bureaus that carefully managed their grants in accordance with applicable standards. For example, in its inspection of the Bureau of Population, Refugees, and Migration, OIG found that the bureau, which oversees a large portfolio of grants and cooperative agreements, developed generally effective internal control policies and procedures for managing these instruments and generally complied with applicable Federal assistance regulations.[29] This bureau had taken substantial steps to improve its processes and had seen genuine change as a result.

Nonetheless, OIG continued to find grants management practices that did not comply with Department requirements. Problems that were noted across multiple inspection reports included missing performance or financial reports; insufficient site visits; improper closeout procedures; and a lack of pre-award evaluation criteria, risk assessments, and monitoring plans.[30] Overlooking formal steps for soliciting, evaluating, monitoring, and documenting grant awards risks using funds on projects that do not match mission priorities or providing funds to grantees that lack the capacity to implement the grant objectives. In another manifestation of this problem, in an inspection of the Bureau of Near Eastern Affairs (NEA), OIG found that a majority of public diplomacy grants reviewed

[28] Department of State, *Agency Financial Report (Fiscal Year 2016)*.

[29] OIG, *Inspection of Bureau of Population, Refugees, and Migration* (ISP-I-17-10, February 2017).

[30] OIG, *Management Assistance Report: Improved Oversight Needed to Standardize the Use of Risk Assessments and Monitoring Plans for Overseas Grants* (ISP-17-33, July 2017); *see also* ISP-I-17-05A, January 2017; ISP-I-17-07A, January 2017; ISP-I-17-08A, January 2017; ISP-I-17-12, May 2017; ISP-I-17-16, May 2017; and ISP-I-17-19, June 2017.

were awarded noncompetitively and without documented justification.[31] Furthermore, most did not have required monitoring and evaluation plans.

The causes of these deficiencies varied, but OIG reports often identified staffing shortages, poor training, and high turnover. Competing priorities also played a role because Grants Officers and Grants Officer Representatives frequently have other responsibilities that are unrelated to oversight of grants. For example, at Embassy Rangoon, 3 staff managed 38 active grants throughout the country in addition to carrying out other responsibilities.[32] The report noted that this was a heavy work load for grants management staff under any circumstance, but it was particularly so in Burma where many of the grants were being implemented in remote locations.

OIG's reports provided recommendations directed at these issues. For example, to guide staff with grants management responsibilities, bureaus and posts should establish and implement formal standard operating procedures for conducting grants management activities that comply with Department requirements.

Ensuring Proper Invoice Review and Approval Processes

Proper invoice review and approval processes are a crucial aspect of ensuring that the Department receives the benefit of its contracts and that the Department is able to take appropriate steps if contractors are not performing appropriately. In FY 2017, OIG issued two audit reports that highlighted domestic bureaus' successful efforts to improve the invoice review and approval process for specific contracts under their purview. OIG reported that NEA developed a standard operating procedure for invoice review and provided invoice examiner training to its staff.[33] These standard operating procedures led, at least in part, to OIG's finding that the percentage of allowable and supported costs approved for payment under the Baghdad Operations and Maintenance Support Services Contract improved over time.[34] Similarly, OIG found that the Bureau of South and Central Asian Affairs established internal controls that complied with applicable invoice review requirements and that the bureau had paid no money in prompt payment interest penalties related to the Afghanistan Life Support Services Contract in FY 2016.[35]

---

[31] OIG, *Inspection of the Bureau of Near Eastern Affairs* (ISP-I-17-22, May 2017).

[32] ISP-I-17-05A, January 2017.

[33] OIG, *Audit of Baghdad Diplomatic Support Center Task Orders Awarded Under Operations and Maintenance Support Services Contract SAQMMA12D0165* (AUD-MERO-17-45, June 2017).

[34] *Ibid.*

[35] OIG, *Audit of the Bureau of South and Central Asian Affairs Invoice Review Process for the Afghanistan Life Support Services Contract* (AUD-MERO-17-47, June 2017).

Again, though, OIG continued to identify ways that the Department could improve its practices. For example, despite implementing a standard operating procedure and training and despite generally following Federal requirements, NEA possessed a significant backlog of invoices that were approved for expedited provisional payment but had not received the required post-payment review. [36] The bureau also failed to properly document its invoice reviews in many cases.[37] Similarly, in an audit of a contract for monitoring services in Iraq, OIG found inadequate supporting documentation for 77 percent of the total amount billed in its sample of invoices.[38] In another example, in an audit of six IT contracts administered by the Bureau of Consular Affairs (CA), Office of Consular Systems and Technology, OIG found that 85 percent of the invoices it reviewed were not approved by the designated Contracting Officer's Representative.[39]

Staffing shortages, high turnover, and a lack of internal controls played a role in these deficiencies, and a number of OIG's recommendations addressed these concerns. For example, OIG recommended that NEA develop and implement a process to periodically review and address staffing requirements in its contract management offices; this recommendation was intended to ensure that invoice oversight staff levels are sufficient to complete effective and timely invoice reviews that comply with Federal requirements and Department guidance.[40] Likewise, OIG recommended that CA's Office of Consular Systems and Technology develop and implement training for its contract oversight staff and put into place internal policies and procedures governing contract administration that specifically include guidance on reviewing and approving invoices.[41]

Monitoring and Documenting Contractor Performance

Over the past several years, OIG has provided the Department with numerous recommendations to improve its oversight of contractor performance, and a 2017 audit report specifically noted that a 2014 management alert had "prompted the Department to improve guidance and training for contract

[36] OIG, *Aspects of the Invoice Review Process Used by the Bureau of Near Eastern Affairs to Support Contingency Operations in Iraq Need Improvement* (AUD-MERO-17-33, March 2017).

[37] *Ibid*.

[38] OIG, *Audit of the Department of State's Contract To Monitor Foreign Assistance Programs in Iraq* (AUD-MERO-17-41, May 2017).

[39] OIG, *Audit of the Bureau of Consular Affairs, Office of Consular Systems and Technology, Administration of Selected Information Technology Contracts* (AUD-CGI-17-38, May 2017).

[40] AUD-MERO-17-33, March 2017.

[41] AUD-CGI-17-38, May 2017.

oversight."[42] OIG identified in its FY 2017 reports several instances in which the Department engaged in appropriate oversight. For example, OIG found that Bureau of South and Central Asian Affairs oversight of the Afghanistan Life Support Services contract was effective. Oversight staff identified and resolved performance issues and reduced invoice payments when contractual requirements were not being fulfilled.[43] The report specifically noted that the Contracting Officers Representatives, "who are Department civil service employees rather than Foreign Service Officers, are dedicated full time to overseeing the . . . contract."[44] Also, OIG reported that CA's Office of Consular Systems and Technology had identified and resolved significant contractor performance issues with some of the contracts OIG audited.[45] In a third report, OIG determined that the Contracting Officers Representatives within DS had made "significant improvements" in file maintenance practices since 2015.[46]

OIG continued to find, however, inadequacies in the monitoring and documentation of contractor performance pertaining to contracts and foreign assistance programs. These deficiencies manifested themselves in various ways, and OIG found concerns in both domestic and overseas operations. For example, OIG detailed ongoing difficulties in monitoring and overseeing the antiterrorism assistance program in Pakistan. In particular, OIG reported that DS had no staff in Pakistan responsible for verifying satisfactory contractor performance or monitoring whether required reports were submitted. Furthermore, the bureau had not adopted a meaningful way to measure progress toward program goals.[47] In another example, an audit of a contract for monitoring services in Iraq reported that the Department did not adequately monitor funds available under contract line item numbers.[48] OIG's inspection reports also highlighted posts where Contracting Officers Representatives served without proper training or without proper designation, which could affect their ability to ensure proper oversight of contractors.[49] Domestically, OIG reported that CA's Office of Consular Systems and Technology contract files did not have all required documentation and that contractor monthly status reports were missing for each contract reviewed.[50]

---

[42] OIG, *Audit of Invoices Submitted by Torres Advanced Enterprise Solutions, LLC, for Select Local Guard Force Contracts* (AUD-CGI-17-63, September 2017) (citing to OIG, *Management Alert (Contract File Management Deficiencies)*, MA-A-0002, March 2014).

[43] AUD-MERO-17-47, June 2017.

[44] *Ibid.*

[45] AUD-CGI-17-38, May 2017.

[46] AUD-CGI-17-63, Sept. 2017.

[47] OIG, *Management Assistance Report: Challenges Remain in Monitoring and Overseeing Antiterrorism Assistance Program Activities in Pakistan* (AUD-MERO-17-37, May 2017).

[48] AUD-MERO-17-41, May 2017.

[49] *See, e.g.*, ISP-I-17-07A, January 2017; ISP-I-17-12, May 2017; ISP-I-17-16, May 2017.

[50] AUD-CGI-17-38, May 2017.

OIG acknowledges that conditions on the ground can have significant effect on the Department's ability to perform oversight. For example, OIG found that difficulty in obtaining visas from the Government of Pakistan was a contributing factor in the Department's flawed oversight and monitoring of the antiterrorism assistance program there.[51] Even in such situations, however, OIG identified specific, practical actions the Department could take to improve oversight, including developing and implementing procedures to verify compliance with contract reporting requirements. In other situations, Department bureaus responsible for administering contracts and foreign assistance should better ensure compliance with contract reporting requirements and should develop and implement monitoring and evaluation systems that measure contractor performance.

INFORMATION SECURITY AND MANAGEMENT

Like all large organizations, the Department depends on information systems and electronic data to carry out its mission. The security of these systems and networks—cybersecurity—is vital to protecting national and economic security, public safety, and the flow of commerce. These same information systems, however, are subject to serious threats, including exploitation and compromise of the information being processed, stored, and transmitted. These threats, in turn, can harm the Department's operations and assets. As described below, OIG's reports have emphasized a number of these risks. OIG also notes that, as discussed in the separate section addressing coordination and the need for clear lines of authority, these issues are affected by the organizational placement of the Chief Information Officer (CIO).

Strengthening Cybersecurity Practices

Overall, during FY 2017, OIG reported that the Department did not have an effective information security program guided by risk-based decision-making, as evidenced by security weaknesses in key IT metrics, including risk management, configuration management, identity and access management, continuous monitoring, incident response, and contingency planning.[52] OIG FY 2017 reports identified various areas where the Department could strengthen its cybersecurity performance. These include Information Systems Security Officer duties, the cybersecurity assessment process, the configuration change control process, and IT contingency planning.

[51] AUD-MERO-17-37, May 2017.

[52] OIG, *Audit of the Department of State Information Security Program* (AUD-IT-17-17, November 2016).

Information Systems Security Officers (ISSO) are responsible for implementing the Department's information systems security program and for working closely with system managers to ensure compliance with information systems security standards. In a management assistance report, OIG reported that one third of its overseas inspections conducted from fall FY 2014 to spring FY 2016 included findings related to the deficient performance of ISSO duties.[53] Similarly, several FY 2017 inspections confirmed that this continued to be a problem for the Department both at overseas posts and domestic bureaus.[54]

Because ISSO duties are often assigned to information management personnel on a collateral basis, competing priorities are sometimes at the root of this challenge. Neglect of these duties, however, may leave the Department vulnerable to cybersecurity attacks. Accordingly, OIG recommended that the Bureau of Information Resource Management (IRM) take the lead in implementing a plan to enforce the performance of ISSO duties by overseas information management personnel in accordance with Department standards.[55] Additionally, OIG issued recommendations for individual overseas posts to implement standard operating procedures to ensure performance of ISSO duties.

OIG also found missed opportunities to improve systems through use of the Department's cybersecurity assessment reports. These reports, which are conducted by DS, focus on cybersecurity practices and include specific recommendations for improvement. In comparing its own reports with DS reports, OIG found that, of the 23 instances in which DS performed a cybersecurity assessment before an OIG inspection of a post, subsequent OIG reports made recommendations reflecting the same or similar deficiencies 18 times.[56] The specific recommendations related to a range of issues, including inadequate performance of ISSO duties, incomplete or untested IT contingency plans, unidentified dedicated internet networks, physical control deficiencies, administrative control weaknesses, and technical control issues. To address this serious issue and to ensure that the Department is taking advantage of its own processes to protect its information security, OIG recommended that the Department require implementation of cybersecurity assessment recommendations and establish a process to track and verify compliance.[57]

---

[53] OIG, *Management Assistance Report: Non-Performance of Information Systems Security Officer Duties by Overseas Personnel* (ISP-17-24, May 2017).

[54] OIG, *Inspection of Consulate General Jerusalem* (ISP-I-17-18, June 2017); ISP-I-17-12, May 2017; ISP-I-17-16, May 2017; ISP-I-17-20, May 2017; ISP-I-17-13, ISP-I-17-22, May 2017, March 2017.

[55] ISP-17-24, May 2017.

[56] OIG, *Management Assistance Report: Deficiencies Reported in Cyber Security Assessment Reports Remain Uncorrected* (ISP-17-39, July 2017). The DS assessments occurred between 1 and 41 months before OIG's inspection, with an average of over 10 months between the two reports.

[57] *Ibid.*

Another report on this subject detailed concerns with the Department's configuration change control process. Configuration change control prevents changes to IT systems or changes that could introduce security weaknesses—such system changes can be as minor as adding a new type of printer or as significant as deploying an entirely new application.[58] At the Department, enterprise change requests must be reviewed through a process led by the Information Technology Configuration Control Board. OIG reported that this board did not authorize or test change requests in compliance with Federal requirements and Department policy. Specifically, change requests were not sufficiently authorized at every stage of the review process, and change requests were not tested as required. As a result of unauthorized and untested change requests, the Department's network, applications, and software are put at risk because of an inconsistently applied and controlled configuration control process.

OIG also continued to find deficiencies in Department IT contingency planning at overseas posts. Department guidelines require every information system to have a contingency plan that is documented and tested annually. Incomplete and untested IT contingency plans increase the risk of ineffective responses to or loss of critical communication during an emergency or crisis. OIG found several embassies that were not (or could not show that they were) testing IT contingency plans annually.[59] For example, OIG found that Embassy Tel Aviv in Israel had not updated its plan annually, which, in turn, meant that managers did not provide initial and annual refresher contingency training to information management personnel.[60] The lack of a properly developed and tested IT contingency plan that is linked with overall emergency preparedness processes could compromise a post's recovery efforts following an IT incident. OIG has accordingly recommended repeatedly that overseas posts conduct IT contingency planning in accordance with Department standards.

Finally, OIG identified inconsistencies and omissions in two databases that track the Department's IT assets.[61] Without accurate and complete information on its IT systems, Department processes meant to protect these systems and safeguard the confidentiality, integrity, and availability of its information are significantly hampered.

---

[58] OIG, *Audit of the Department of State's Information Technology Configuration Control Board* (AUD-IT-17-64, September 2017).

[59] *See, e.g.*, OIG, *Inspection of Embassy Accra, Ghana* (ISP-I-17-17, June 2017); ISP-I-17-18, June 2017; ISP-I-17-12, May 2017; ISP-I-17-13, March 2017; ISP-I-17-19, June 2017.

[60] ISP-I-17-20, May 2017.

[61] OIG, *Management Assistance Report: The Process to Authorize and Track Information Technology Systems Needs Improvement* (AUD-IT-17-56, August 2017).

Establishing Effective Records Management Programs

In a number of FY 2017 inspections, OIG noted Department entities that were not fulfilling records management responsibilities. For example, NEA did not have an active records management program with adequate guidance regarding creation, maintenance, use, and disposition of records.[62] OIG also found several embassies that had ineffective records management programs and employees who were untrained on records management responsibilities.[63] Similarly, OIG inspections reported that, at a number of embassies, employees did not consistently use record emails to document activities and operations.[64] Finally, with respect to paper records, OIG noted poor practices in two inspections in which it observed safes containing classified documents from departed employees that were not retired, archived, or disposed.[65]

Inattentive management, a lack of employee training, and unclear existing guidance are contributing factors in these deficiencies. To address these issues, OIG has recommended that Department entities establish records management programs that are in accordance with Department guidance and that include dedicated and trained staff with records management responsibilities. Posts and bureaus should also prescribe and adhere to internal guidance for maintaining files and records and train employees on the appropriate use of record emails.

FINANCIAL AND PROPERTY MANAGEMENT

Financial management has historically been a challenge for the Department, and, as described below, OIG continued to identify concerns related to this issue. OIG has modified this challenge from previous management challenges reports to include the related issue of property management because OIG's work this year repeatedly identified the difficulties the Department faced in managing both financial issues and its property. This challenge, in particular, implicates a wide range of Department functions and management practices. One significant aspect of this challenge relates to overall internal control issues—namely, the Department's ability to identify internal control weaknesses in the first place and the Department's subsequent compliance with relevant standards. This issue affects management of both the Department's financial resources and its property. This section also describes the Department's difficulties in tracking and reporting data affecting financial issues, especially foreign assistance. In addition, we identify weaknesses in the Department's collection, use, and analysis of financial information. Finally, this section

[62] ISP-I-17-22, May 2017.

[63] *See, e.g.*, ISP-I-17-12, May 2017; ISP-I-17-16, May 2017.

[64] OIG, *Inspection of Embassy Colombo, Sri Lanka* (ISP-I-17-14, April 2017); ISP-I-17-13, March 2017; ISP-I-17-16, May 2017; ISP-I-17-12, May 2017.

[65] ISP-I-17-16, May 2017; ISP-I-17-14, April 2017.

discusses areas where the Department has not effectively sought reimbursement for services provided or implemented cost-sharing measures. As with oversight of contracts and grants, attention to this challenge is particularly important to ensure that the Department appropriately oversees and uses taxpayer resources.

Identifying Internal Control Deficiencies

Effective management control systems play a key role in ensuring that the Department is able to achieve its objectives through effective stewardship of public resources. The Department's statement of assurance process—in which Department entities (including bureaus, special offices, and overseas missions) submit annual statements of assurance—partially informs the Secretary of State's opinion regarding the effectiveness of the management controls and the existence of any material weaknesses or significant deficiencies.

In FY 2017 inspections of overseas posts and domestic bureaus, OIG continued to find deficiencies in the statement of assurance process. In numerous inspections, OIG found recent statements of assurance in which the entity being inspected had identified no or very few internal control deficiencies. Upon inspection, however, OIG found numerous deficiencies that had been overlooked.[66] For example, in one inspection of an overseas post, OIG found 22 internal control deficiencies despite the embassy's 2016 statement of assurance that identified no deficiencies.[67] Furthermore, one bureau did not prepare written standard operating procedures for the annual exercise.[68]

OIG noted management's important role with respect to this issue. In a report that reviewed findings in 34 inspection reports on overseas missions issued from December 2014 through January 2017, OIG examined its findings regarding chief of mission and deputy chief of mission performance in five areas, including adherence to internal controls.[69] OIG reported that 38 percent of inspections had found deficiencies in the chief of mission's oversight of embassy internal controls and the annual statement of assurance process.

Weak internal controls that go unidentified by management increase the risk of misuse of Department resources. Each Department entity plays a role in formulating the Department's annual statement of assurance and should, therefore, ensure that vulnerabilities in the process are identified and appropriate corrective actions are taken. The Department should include

[66] *See, e.g.*, ISP-I-17-19, June 2017; ISP-I-17-12, May 2017; ISP-I-17-16, May 2017; ISP-I-17-07A, January 2017.

[67] ISP-I-17-16, May 2017.

[68] ISP-I-17-10, February 2017.

[69] ISP-17-38, July 2017.

additional training on management control responsibilities in its classes for chiefs of mission and deputy chiefs of mission.

Complying With Internal Controls

In many FY 2017 inspections, OIG found internal control deficiencies that spanned a wide range of operations, including functions related to financial and property management. Numerous inspections found deficiencies in cashier operations, which were related to periodic reconciliations, unannounced verifications, and separation of duties, among others.[70] OIG also found persistent problems with procurement. One post, for example, failed to maintain separation of duties in ordering, receiving, billing, and paying for goods and services.[71] OIG also noted several examples of posts that failed to establish acquisition plans, which, when used effectively, decrease the risk that staff will procure unnecessary goods and services.[72] All of these practices put the Department's financial resources at risk.

Another example of internal control weaknesses was identified in the annual audit of the Department's financial statements. There, an external auditor performing the audit on OIG's behalf and under OIG's direction identified a significant number of invalid unliquidated obligations (ULOs)[73] that had not been identified by the Department's own review process. This occurred, at least in part, because the internal control structure was not operating effectively to comply with existing policy or to facilitate the accurate reporting of ULO balances in the financial statements. In particular, the Department's internal controls were not effective to ensure that ULOs were consistently and systematically evaluated for validity and deobligation.[74]

Internal control deficiencies related to property management were also wide-ranging. Several reports noted particular issues with fuel. For example, OIG found that several posts failed to properly secure and control access to their bulk fuel inventory, did not perform spot checks of fuel deliveries, or did not calibrate pumps and tanks.[75] This problem extended to residential properties

---

[70] *See, e.g.*, ISP-I-17-12, May 2017; ISP-I-17-13, March 2017; ISP-I-17-16, May 2017; ISP-I-17-05A, January 2017; and ISP-I-17-14, April 2017.

[71] ISP-I-17-14, April 2017.

[72] ISP-I-17-12, May 2017; ISP-I-17-16, May 2017; ISP-I-17-11A, February 2017.

[73] Unliquidated obligations represent the cumulative amount of orders, contracts, and other binding agreements for which the goods and services that were ordered have not been received or the goods and services have been received but for which payment has not yet been made.

[74] OIG, *Audit of the Department of State's FY 2016 and FY 2015 Financial Statements* (AUD-FM-17-09, November 2016).

[75] ISP-I-17-14, April 2017; ISP-I-17-12, May 2017; ISP-I-17-16, May 2017; ISP-I-17-17, June 2017; and ISP-I-17-19, June 2017.

leased by the Department. In one report, OIG determined that safeguards meant to protect residential fuel tanks at diplomatic residences in Amman, Jordan were easily circumvented and that additional vulnerabilities in fuel tank and boiler rooms could leave embassy residences susceptible to diesel fuel loss.[76] Because of the significant value and widespread threats of theft of this commodity, fuel is a particularly vulnerable asset.

In another audit, OIG found that the Department did not maintain sufficient accountability over the inventory of armored vehicles stored domestically. Specifically, Department data on armored vehicles in the inventory systems was not always accurate and five vehicles could not be located during a physical inventory. A single armored vehicle can cost more than $100,000. Without sufficient controls, vehicles could be misappropriated, which could have a significant financial effect on the Department.[77]

In terms of general physical inventories, some posts did not strictly control access to areas where supplies and stock were kept, failed to ensure supplies were issued for official use only, and neglected to perform periodic inventories and reconciliation of property records.[78] Separation of duties was again an issue, with one post using the same personnel to receive, record, and tag incoming assets.[79] All of these issues increased the risks that Department property might be misappropriated or diverted.

Tracking and Reporting Department Assets

Throughout this reporting period, OIG identified weaknesses in the Department's ability to keep track of and report its assets. OIG considers this to be a manifestation of weaknesses in financial and property management because, without an accurate understanding of its assets—financial or otherwise—the Department cannot adequately account for, much less use effectively, those resources. This is an issue that overlaps with internal controls deficiencies.

In some instances, these weaknesses were identified in the course of work that addressed other issues. For example, in an evaluation that focused on the timeliness and cost-effectiveness of the Department's security clearance process, OIG found that the Department does not have accurate information regarding the costs of conducting a security clearance. This, in turn, makes it

[76] OIG, *Management Assistance Report: Additional Measures Needed at Embassy Amman to Safeguard Against Residential Fuel Loss* (AUD-MERO-17-50, July 2017).

[77] AUD-SI-17-21, February 2017.

[78] ISP-I-17-12, May 2017; ISP-I-17-08A, January 2017.

[79] ISP-I-17-05A, January 2017.

difficult to assess the cost-effectiveness of its processes or to accurately bill other agencies for overseas investigatory work that it performs on their behalf.[80]

Perhaps the most notable example of this problem is the challenge that the Department faces in tracking and reporting on foreign assistance funds. As highlighted in a compliance follow-up review, even though OIG issued a recommendation on this issue some time ago, the Department's tracking and reporting processes are still inadequate.[81] The lack of information on this crucial aspect of the Department's work hinders its ability to manage foreign assistance resources strategically, identify whether programs are achieving objectives, and determine how well bureaus and offices implement foreign assistance programs. The significance of this problem is illustrated by the fact that Congress limited the Department's ability to use certain appropriated funds until it submitted a plan to address OIG's recommendations on the issue.[82]

Collecting, Analyzing, and Using Financial Information

A number of OIG reports identified flaws in the Department's collection, use, and analysis of financial information. Although OIG's work in this area tended to address specific programs or bureaus, OIG views this as an overall financial management challenge because of the common threads in these reports—namely, the use of outdated or otherwise weak methods of collecting, analyzing, and applying financial and related data. We have noted similar concerns in the past[83] and discuss below two particularly important examples of this issue described in FY 2017 reports.

First, OIG reported significant flaws in the Department's processes that set certain cost-of-living allowances for Department employees who are stationed in foreign areas.[84] Although OIG identified weaknesses in the calculation of all of the allowances audited, the report particularly identified flaws in setting the post allowance, which is intended to ensure that employees are not financially penalized for working at a more expensive overseas location. OIG's report described a laborious, subjective, and error-prone process for gathering data that has not changed in decades. The flaws in this data gathering process, in

[80] OIG, *Evaluation of the Department of State's Security Clearance Process* (ESP-17-02, July 2017).

[81] OIG, *Compliance Follow-up Review: Department of State is Still Unable to Accurately Track and Report on Foreign Assistance Funds* (ISP-C-17-27, June 2017).

[82] Consolidated Appropriations Act, 2017, HR 244-486, § 7006, available at https://www.congress.gov/115/bills/hr244/BILLS-115hr244enr.pdf.

[83] *See, e.g.*, OIG, *Audit of the Financial Results of the Telephone, Wireless, and Data Cost Center* (AUD-FM-16-32, March 2016); OIG, *Audit of Selected Working Capital Fund Cost Center Financial Results* (AUD-FM-13-36, September 2013).

[84] OIG, *Audit of Select Cost-of-Living Allowances for American Employees Stationed in Foreign Areas* (AUD-FM-17-51. Aug. 2017). Between FY 2013 and FY 2015, the Department spent approximately $673 million on the three allowances addressed in the report.

turn, led to substantive errors in the allowances themselves. OIG recommended that the Department use independent economic data instead of collecting this information on its own; OIG estimated that doing so would have saved more than $18 million between FY 2013 and FY 2015 at six of the seven posts audited.

Second, OIG identified significant flaws in the processes CA used to set fees for selected consular services.[85] The external auditor performing the audit on OIG's behalf and under OIG's direction found that CA collected consular fees of $3.7 billion during FY 2014 and $4.1 billion during FY 2015 but that the cost of providing the relevant services was only $3.3 billion each year. Consequently, the report explained that CA did not comply with Office of Management and Budget Circular A-25, which governs user charges, and relevant fee-governing statutes.

The report identified two reasons that this occurred. First, the price of one fee was not adjusted even though the cost of providing the service had decreased. The report noted that, as of FY 2013, CA did not receive an appropriation to cover certain costs and that CA needed additional funds. By not reducing this fee, CA collected revenue that offset some of the lost funding. As noted in the report, however, CA does not have the legal authority to take this approach and was instead required to set fees at the cost of providing the underlying services.[86] Second, CA more generally used a flawed fee-setting methodology that did not rely on adequate data and did not fully consider the effects of large carry-forward balances—at the beginning of FY 2017, for example, CA had a total unobligated balance from consular fees of almost $1.4 billion. Further, CA did not have an adequate process to analyze its financial results over time to determine whether adjustments were required to its fee-setting methodology, and it did not have adequate historical data or sound quality processes to assess the data that it did use. OIG recommended the Department return $284 million in excess unobligated balances from consular fees to the Department of the Treasury to be put to better use across the Federal Government and to benefit taxpayers. OIG also recommended the Department develop and implement standard data documentation and quality control measures.

Seeking Reimbursement and Sharing Costs for Services Provided

Finally, OIG inspections reported weaknesses in various methods by which the Department should ensure that costs are appropriately shared across agencies. As noted above, the Department does not maintain information necessary to

[85] OIG, *Audit of the Bureau of Consular Affairs Fee-Setting Methodology for Selected Consular Services* (AUD-FM-17-53, September 2017). CA charges fees for many of its services and is permitted to retain funds generated from some of those fees. Other fees, however, must be remitted to the Department of the Treasury.

[86] OMB Circular A-25, "User Fees," July 8, 1993.

ensure that it can accurately bill for overseas investigatory work it performs on other agencies' behalf.[87] In addition, OIG reported that the Department did not appropriately designate particular positions to the International Cooperative Administrative Support Services (ICASS) system so that other agencies that received services from those positions shared the cost of providing them. In particular, OIG identified 52 U.S. direct-hire information management positions whose salary and benefits costs were being paid entirely by the Department even though other agencies used these services at various diplomatic and consular posts overseas.[88] Because other agencies are benefiting from these individuals' work, their salaries should be paid through the ICASS Working Capital Fund, a mechanism for spreading the cost among Federal agencies at overseas posts. OIG estimated the Department could recover $81,331 per position, or a total of $4.23 million annually, if it converted these 52 information management positions to ICASS.

OPERATING IN CONTINGENCY AND CRITICAL ENVIRONMENTS

In FY 2017, the Department continued to carry out programs and operations in environments affected by ongoing "contingency operations" (involving the deployment of the U.S. military overseas) and in what the Department calls "critical environments" (other situations characterized by conflict, instability, and natural disasters, including disease). Recognizing the particular difficulties of managing posts and programs in such areas, as well as the fact that the Department has spent billions of dollars doing so, OIG continued to focus closely on the complex issues affecting Department operations in these environments. The difficulties of these operations often contribute to the management and performance challenges discussed elsewhere in this report.

Managing contracts and grants can be particularly challenging in these locations, and many OIG reports related to contingency and critical environments focused on this issue quite closely. For example, an audit of the Baghdad Life Support Services and Operations and Maintenance Support Services[89] contracts in Iraq illustrates the unique challenges associated with the administration of large, complex contracts in such areas. Among other

[87] ESP-17-02, July 2017.

[88] *Management Assistance Report: Cost of Information Management Staff at Embassies Should Be Distributed to Users of Their Services* (ISP-17-23, May 2017).

[89] As relevant to this discussion, the Baghdad Life Support Services contract addresses acquisition, inspection, and delivery of fuel and has a not-to-exceed cost of $1 billion. As relevant to this discussion, the Operations and Maintenance Support Services contract addresses testing, storage, and distribution of fuel as well as maintenance of fuel-related equipment for all sites in Iraq. It has a not-to-exceed cost of $2 billion.

conclusions, OIG found that NEA had not assigned personnel with the contract management and technical experience to oversee these contracts.[90] Inexperience was compounded by 1-year rotations, which allow limited time to understand and oversee the contract, particularly in light of the fact that, on average, 17 percent of that rotation is spent on rest and recuperation travel. As a result, many oversight activities did not occur, and subpar contractor performance went unaddressed.[91]

OIG's report addressing the operations and maintenance contract at Embassy Kabul also identified the relationship among staffing limitations, security concerns, and contract oversight. Here, OIG determined that the contract did not contain clear, specific, and measurable performance metrics. OIG noted that remedying these deficiencies was "paramount" in posts such as Kabul. Because staff are assigned to 1-year rotations, "the learning curve for managing a large and complex contract is high, and the staff have to respond to continuous threats against and changes at the embassy."[92] In the same report, OIG found that the Contracting Officer had not assigned an alternate Contracting Officers Representative, which created oversight gaps that were particularly concerning in this security environment. For example, the report described an instance in which someone without authorization to do so approved a change in offloading fuel tanks necessitated by "safety and security concerns" because of the Contracting Officer Representative's unavailability.[93]

In another example, OIG's report addressing oversight of the antiterrorism assistance program in Pakistan focused on the unique staffing challenges associated with work in this location. In particular, OIG found that difficulty in obtaining visas for oversight personnel contributed to the Department's inadequate oversight of this program.[94] OIG also identified ways that the Department's own practices contributed to problems, notwithstanding the fact that oversight personnel could not be located in Pakistan. For example, the Contracting Officer waived—without formally modifying the terms of the contract—many reporting requirements that would have allowed the Department to verify satisfactory contractor performance. OIG accordingly recommended that the Department develop and implement procedures to confirm compliance with contract reporting requirements; OIG also recommended that, in situations where the operating environment warrants a

---

[90] OIG, *Audit of the Oversight of Fuel Acquisition and Related Services Supporting Department of State Operations in Iraq* (AUD-MERO-17-16, December 2016).

[91] *Ibid.*

[92] OIG, *Management Assistance Report: Contract Management—Lessons Learned from Embassy Kabul, Afghanistan, Operations and Maintenance Contract* (AUD-MERO-17-04, October 2016).

[93] *Ibid.*

[94] AUD-MERO-17-37, May 2017.

contract modification, Department personnel with oversight responsibility should execute such modifications in line with appropriate guidelines.

OIG notes, though, that the challenges associated with contingency environments are not limited to those pertaining to contracts and grants. In the inspection of Mission Pakistan, OIG concluded that the mission's security policies restricting staff travel in country made it difficult to meet with Pakistani contacts and audiences; this, in some cases, impeded operations or program implementation.[95] For example, the types of public diplomacy programs the Public Affairs Section conducted were necessarily constrained—although OIG noted that the section made innovative use of exchange program alumni and virtual programming to work around this limitation. The inspection report also noted that travel restrictions were partly to blame for a backlog of immigrant visa fraud investigations.

Other OIG inspections also revealed the unique obstacles affecting work in unstable environments. The inspection of Embassy Monrovia in Liberia served as an example of how a difficult operating environment can contribute to and exacerbate weaknesses in internal controls at an embassy. Management staff there stated that the strain the Ebola crisis put on the mission in 2014 and 2015 was at the root of a wide range of problems that included everything from driver certifications, collection of travel advances, spot checks of inventory, and grants management procedures.[96]

The OIG inspection of Embassy Freetown in Sierra Leone further illustrated the effect of the Ebola crisis on Department programs and operations.[97] As in Monrovia, the crisis strained the embassy's internal controls, and during the inspection, OIG identified numerous and significant deficiencies in facility maintenance and security. Furthermore, OIG found the Consular Section was still working to address associated problems, including eliminating immigrant visa genetic testing backlogs and rebuilding the consular warden system. The embassy's focus on responding to the Ebola crisis—including dealing with an influx of funding and additional U.S. Government personnel when staff was already short in certain embassy sections—hampered its ability to attend to ordinary operational functions.

WORKFORCE MANAGEMENT

The Bureau of Human Resources rightly identifies staff as the Department's greatest asset. The Department accordingly expends substantial resources on recruiting, training, and retaining a diverse, talented workforce capable of

[95] ISP-I-17-11A, February 2017.

[96] ISP-I-17-12, May 2017.

[97] ISP-I-17-16, May 2017.

carrying out the Department's foreign policy goals and priorities. Across functional areas and geographic regions, however, OIG's work finds that inexperienced staff, insufficient training, and staffing gaps and frequent turnover contribute to the Department's other management and performance challenges. These problems afflict programs and operations domestically and overseas and are identified in a range of reports that cover a variety of topics.

For example, as described previously, OIG issued a report that identified numerous physical deficiencies on two buildings constructed at Embassy Kabul.[98] OIG noted that these deficiencies were in large part a result of poor quality assurance and oversight of the construction process. OIG's report specifically commented that the lack of an adequate number of qualified quality assurance staff contributed to these problems. For example, OIG found that some of the Department's quality assurance staff did not take the opportunity to conduct physical inspections and signed off on items that were never inspected. OIG also identified the project director's failure to make full use of the subject-matter experts that OBO had retained to observe, oversee, and document the functional performance of building systems to verify that these systems met design intent and contract requirements. In another report, OIG noted that personnel responsible for overseeing contracts related to fuel acquisition in Iraq lacked contract-administration experience and technical expertise. OIG concluded that this lack of experience contributed to oversight deficiencies leading to millions of dollars in questioned costs stemming from fuel purchases that did not conform to quality standards specified in the contract.[99]

In another example, OIG found that contract administration within CA's Office of Consular Systems and Technology was affected by the lack of training on contract administration policies for Contracting Officers Representatives and Government Technical Monitors; this same report found that more senior personnel did not sufficiently appropriately oversee Contracting Officers Representatives and Government Technical Monitors.[100] In another report, OIG identified a range of problems associated with allocation, tracking, and maintenance of armored vehicles.[101] OIG specifically recommended that DS hire an "experienced program manager who has an expert knowledge of internal controls and vehicle fleet management experience" to manage the fleet. The report noted that the then-current branch chief position was typically a rotating Foreign Service position and

[98] AUD-MERO-17-44, June 2017. In addition to the fire and electrical concerns noted previously, these physical deficiencies included plumbing systems; heating, ventilation, and air conditioning systems; and elevators.

[99] OIG, *Audit of the Oversight of Fuel Acquisition and Related Services Supporting Department of State Operations in Iraq* (AUD-MERO-17-16, December 2016).

[100] OIG, *Audit of the Bureau of Consular Affairs, Office of Consular System sand Technology, Administration of Selected Information Contracts* (AUD-CGI-17-38, May 2017).

[101] AUD-SI-17-21, February 2017.

that the person holding the position typically had the technical background necessary to manage the security aspects of the program but was not required to possess specialized skills necessary for the fleet management aspects of the program.

OIG also identified other workforce management concerns. For example, OIG's inspection of NEA found that this bureau attracted the fewest number of bidders for its domestic positions of any of the regional bureaus, and approximately 75 percent of its overseas positions were designated as hard-to-fill. This places at risk NEA's ability to develop the next generation of diplomats with expertise in the region. On a related point, OIG noted that NEA's growing workload in parts of the bureau combined with understaffing led to workplace stress and employee burnout.[102]

These poor workforce practices have real, practical implications for the Department. Remedying physical deficiencies at the two new buildings at Embassy Kabul could cost the Department millions of dollars, and widespread inadequacies in the oversight of contracts and grants increases the risk of fraud, waste, and abuse of Government resources.

PROMOTING ACCOUNTABILITY THROUGH INTERNAL COORDINATION AND CLEAR LINES OF AUTHORITY

Promoting accountability through careful, internal coordination and clear, well-defined lines of authority is crucial. OIG, however, has identified program management weaknesses associated with a lack of coordination and dispersed authority as a serious challenge facing the Department. This is a concern that is reflected in a wide range of OIG's reports. OIG has included this as a management challenge because of its significant implications for the Department's ability to implement its programs and operate efficiently and effectively. Moreover, as described below, unclear lines of authority and a lack of coordination have particular consequences for both physical and IT security.

OIG acknowledges that, in some areas, the Department has made efforts to address these concerns. To take just one example, OIG's inspection of NEA discussed the ways that the bureau worked across "complex lines of authority" to address a range of crises in its area of operations and noted that it complied with Department guidance requiring it to serve "as the single focus of responsibility for leadership and coordination" of government activities in "its area of assignment." In the same report, OIG highlighted the effective coordination work of two NEA offices—the Office of Iranian Affairs and the Office of Maghreb Affairs. OIG, however, identified other areas where

[102] ISP-I-17-22, May 2017.

coordination was not effective, noting, for example, that NEA did not fully engage with the Bureau of Conflict and Stabilization Operations, although the two bureaus had overlapping responsibilities in some areas.[103]

Moreover, in other specific program areas, challenges regarding coordination and clear lines of authority persisted. For example, OIG identified ineffective administration of the armored vehicle program that resulted, in part, from a lack of documentation and understanding regarding the relative roles of DS and the Bureau of Administration.[104] Confusion over its role in the program contributed to DS's failure sufficiently to oversee the program and strategically plan the allocation of armored vehicles at overseas posts.

Another area of concern is the lack of coordination between OBO and DS, both of which have responsibilities for physical security of diplomatic facilities. Although OBO and DS collaborate on a number of working groups, OIG has long pointed out the implications of this overall lack of coordination and encourages complete implementation of its recommendation for these bureaus to work together to develop formal, standardized processes to prioritize physical security-related deficiencies at posts by category.[105] One recent example of the consequences of a lack of coordination concerns a gap OIG identified in the security certification process. In particular, OIG found that the improper alterations on security doors were overlooked, in part, because the security certification process did not include a follow-up inspection by DS to confirm that OBO's actions to address identified physical security deficiencies were in accordance with physical security standards.[106]

OIG has also identified concerns regarding overlapping and poorly defined information security responsibilities between DS and IRM.[107] The Federal Information Technology Acquisition Reform Act enhanced the CIO's authority and responsibility for the implementation of an agency's information security program. According to Department policies, however, both IRM and DS have responsibilities for information security, even though the Department's CIO, who is the head of IRM, should have this role. Furthermore, the Department's current organizational risk-reporting structure requires the CIO and DS separately to

---

[103] *Ibid*.

[104] AUD-SI-17-21, February 2017.

[105] OIG, *Compliance Follow-up Audit of the Process To Request and Prioritize Physical Security-Related Activities at Overseas Posts* (AUD-ACF-16-20, December 2015); OIG, *Management Assistance Report: Department Attention Needed to Address Overdue Responses on Selected Open Recommendations* (AUD-ACF-17-55, July 2017).

[106] AUD-MERO-17-28, March 2017.

[107] *See, e.g.,* OIG, *Audit of the Department of State's Efforts to Detect and Address the Use of Unapproved Portable Devices* (AUD-IT-17-61, September 2017) and AUD-IT-17-17, November 2016.

report to the Under Secretary for Management; DS and other bureaus or offices reporting to the Under Secretary for Management, however, are not required to communicate information security risks to IRM. In 2015, OIG recommended that the Department review the organizational placement of the CIO to address this decentralized risk-reporting structure.[108] The Department acknowledged the need for enhancements to information security across the Department, but it determined that the CIO's position within IRM was sufficient to implement an effective agency-wide information security program. The Department stated that it had instead made efforts to improve the effectiveness of its information security program by drafting a new approach to managing information system-level security risks. As a result, the CIO is still not organizationally placed to address information security program issues effectively.

A recent report illustrates the flaws in this organizational structure. In particular, OIG reported that insufficient program management was one reason that the Department did not authorize or test IT change requests in accordance with Department and Federal policies. The report explained that, although IRM is responsible for ensuring control over change requests, the CIO, who is located within IRM, does not have sufficient authority to manage activities of the Information Technology Configuration Control Board, as provided for in law. This relative lack of authority increases the need for a strong, centralized, oversight function within IRM to ensure that changes requested for IT systems are safe and will not damage the Department's IT infrastructure and also to ensure consistent implementation of Office of Management and Budget requirements. The Department, however, has not established and implemented such an oversight function to allow IRM to perform this role appropriately under the current organizational structure. To the contrary, IRM management stated that IRM's role was to facilitate the change request process rather than to act as a program manager for the process.[109]

CONCLUSION

Each of the management challenges described in this report has an effect on the Department's ability to perform its mission and to safeguard taxpayer resources while doing so. As such, each challenge independently warrants ongoing attention.

OIG notes as well the unique vulnerabilities that emerge when these challenges interact with one another. They do not exist in isolation; rather, many overlap with and exacerbate one another. For example, operating in contingency and critical environments amplifies the Department's weaknesses in managing

[108] OIG, *Audit of the Department of State Information Security Program* (AUD-IT-16-16, November 2015).

[109] AUD-IT-17-64, September 2017.

contracts and grants. The already challenging task of overseeing and monitoring a complex foreign assistance program becomes even more challenging when the Department cannot put oversight staff on the ground where a particular program is being implemented. An additional example pertains to information security, where weaknesses can have a broad effect on the Department and worsen challenges such as financial management. In particular, IT security weaknesses can affect the integrity of financial applications, which, in turn, increases risks that sensitive financial information could be accessed by unauthorized individuals, that financial transactions could be accidentally or intentionally altered, or, more basically, that the Department will be unable to report financial data accurately. OIG accordingly encourages the Department to consider the ways that these challenges compound each other and how it can address these problems systematically rather than in a piecemeal fashion.

APPENDIX A: RESPONSE FROM THE DEPARTMENT OF STATE

In 2017, the Department of State's Office of Inspector General (OIG) identified management and performance challenges in the areas of: protection of people and facilities; oversight of contracts, grants, and foreign assistance; information security and management; financial and property management; operating in contingency and critical environments; workforce management; and promoting accountability through internal coordination and clear lines of authority. The Department promptly takes corrective actions in response to OIG findings and recommendations. Highlights are summarized below.

Protection of People and Facilities

The protection of people and facilities remains a top priority for the Department. In a very dangerous world, the Department is succeeding in keeping its personnel and facilities safe. Threats to our people and facilities will continue to evolve and requires constant focus and risk mitigation. To manage risk, the Department is developing its Enterprise Risk Management program. The Department annually revises the Security Environment Threat List and conducts High Threat Post Review Board assessments, and it is increasing the number of posts for which the Foreign Affairs Counter Threat training is mandatory. Despite these and other efforts, the challenge of eliminating risk and preventing attacks will continue given the nature of diplomacy and the environment.

Below is additional information about specific issues raised by the OIG and improvements the Department has made in its systems for protecting people and facilities.

- In response to evolving threats, the Department developed and implemented a mandatory High Threat Security Overseas Seminar training course for contractors to take prior to their deployment to contingency operation posts and critical environments.
- The Department disagrees with OIG's assertion that poor quality assurance and oversight of the construction process of two buildings at Embassy Kabul led to failure to adhere to electrical and fire safety standards.
    - The company that was consulted on these deficiencies had a conflict of interest. It was actively negotiating a maintenance contract with the U.S. Government and could have benefitted from identifying maintenance issues that required mitigation.
    - OIG conducted this audit during the warranty period. The majority of construction issues noted in the report are being

mitigated by the contractor. The OIG is not following standard operating procedures in conducting an audit during an active construction project.

- The Department took steps to address issues OIG identified involving the maintenance of armored vehicles. The Department implemented an enhancement of the Fleet Management Information System (FMIS), which allows maintenance work orders to be created and tracked and captures maintenance data for domestically located armored vehicles. In addition, the FMIS system has been configured to alert and/or remind users that preventative maintenance is due or overdue.

Oversight of Contracts, Grants, and Foreign Assistance

In response to OIG recommendations, the Department took a number of actions to improve oversight of contracts and grants, including those that appear below. The Department will continue to take steps to address the recommendations.

- The Department is developing online training that explains risk assessments and monitoring plan requirements for grants and cooperative agreements. The training is anticipated to be available in May 2018.
- Embassy Rangoon's Political/Economic Section's Small Grants Program completed closeout for 42 expired grants from three previous fiscal years. Remaining funds were de-obligated and/or returned to the Embassy by the grant recipients, resulting in a zero balance.
- The Bureau of Consular Affairs developed a Contract Monitoring and Administration Quick Guide, which reinforces and enhances existing policy and procedures governing contract administration. The guide also includes a newly developed Risk Management and Compliance Program section to assure Contract Officer Representatives and Government Technical Monitors are held accountable for meeting all responsibilities delegated to them by the Contracting Officer. The guide is pending final approval.

Information Security and Management

The Department recognizes the significant threats that exist to its information systems and is constantly taking actions to reinforce its defenses against those threats.

- The Department developed a Cybersecurity Strategy Framework for fiscal years 2017-2019. It will provide an operational framework that enhances the Department's cybersecurity defense-in-depth information assurance program.

- The Department began an unprecedented drive to close its backlog of Freedom of Information Act cases within a period of months.
- The Department instituted an email management system at the end of 2016 that includes a centralized repository for the vast majority of Department email records. These OpenNet and ClassNet emails are automatically captured, retained, and disposed of in accordance with their appropriate disposition.
- The Department is in the final stages of updating the required records management training course. This revamped distance-learning course will be available in March 2018. The Department tracks compliance with records training.
- The Enterprise Risk Management Work Group initiated a comprehensive initiative to streamline the Department's 6,700 records disposition schedules.

Financial and Property Management

The Department operates in a complex and challenging global environment. As a result, the Department manages one of the U.S. Government's most complex financial operations. Operating around-the-clock in over 270 locations and 180 countries, we conduct business in over 135 currencies, account for $100 billion in assets, maintain 225 bank accounts around the world, execute over 6,000 annual foreign currency purchases and sales valued at over $4 billion, and manage real and personal property capital assets with historical costs of more than $34 billion.

Department officials at all levels, both at home and abroad, are dedicated to ensuring effective management controls and oversight over the resources entrusted to the Department. In doing so, the Department has received five consecutive unmodified opinions (FY 2012-2016) from the external Independent Auditor on our annual Department-wide financial statements. In addition, the Department ended FY 2016 with no reported material weaknesses in internal controls over financial reporting. Last year, in recognition of the exceptional quality of the Department's Agency Financial Report, the Association of Government Accountants awarded the Department the prestigious Certificate of Excellence in Accountability Reporting.

The following are examples of improvements in response to OIG recommendations as well as additional information about a recommendation with which the Department disagrees:

- The Department disagrees with OIG's assertion that the Statement of Assurance (SoA) process itself is deficient, but agrees that improvements in posts' reporting of deficiencies through other means are needed. Improvements made to the SoA process included updating and

expanding the Management Controls Checklist that was distributed to Assistant Secretaries and Chiefs of Mission, providing in-person training to Bureau Management Control Coordinators, providing SoA training to a Post Management Officer course at the Foreign Service Institute and to managers in the Arms Control and International Security bureaus during 2017. In addition, the Bureau of Population, Refugees and Migration disseminated a risk management policy and program review memorandum that includes standard operating procedures for the annual SoA.

- The Department worked to update the content on management control responsibilities for its Ambassadorial Seminar and its Deputy Chief of Mission/Principal Officers' Seminar.
- The Department initiated a strategic review of the International Cooperative Administrative Services System (ICASS). As part of the review, the Department is identifying services that support the ICASS platform that could be realigned into ICASS, rather than being funded exclusively by the Department or direct-charged to agencies.
- The Department uses several tools to actively monitor cashiering operations, including cashier system controls and an oversight cashier monitor function carried out by the Bureau of the Comptroller and Global Financial Services (CGFS). Cashier Monitors review post cashier transactions and work to ensure compliance with monthly unannounced cash counts and reconciliations of the Cashier's accountability performed by the Foreign Service Financial Management Officer or the Management Officer at each Post. CGFS measure posts' performance with this compliance on a monthly basis and has developed an annual Cashier Operations Based Risk Assessment tool to help prevent theft, fraud and misuse of cash within the operations deemed higher risk. The tool analyzes operational risk, verification and controls and an overall cashier operation assessment. CGFS also conducts on-site reviews of all Class B Cashier operations at least every five years, which provides an in-depth history of operations and post actions on findings.
- Improving the reporting to the American public on how the Department spends their tax dollars is a priority goal for the Department. The Digital Accountability and Transparency Act of 2014 (DATA Act) requires agency financial and payment information to be reported to the public using USASpending.gov in accordance with Government-wide financial data standards. As required under the Act, on April 30, 2017, the Department made its first submission of the requisite data files on Department spending for the second quarter of FY 2017 to the DATA Act Broker.
- The Department disagrees with OIG's assertion that the Bureau of Consular Affairs (CA) set its fees based on inaccurate data and should remit to the Department of the Treasury (Treasury) unobligated balances

that exceed the carry forward threshold and could be put to better use for FY 2017.

  - Consular fees were established in accordance with statutory and regulatory authorities and, therefore, there is no requirement to remit the funds to the Treasury. Furthermore, it is unclear what legal authority the Department would rely on to return fees to the Treasury, which Congress has explicitly authorized the Department to retain until expended.
  - Consular fee setting is a multi-year process subject to changes in rulemaking, which is why consular fees are typically updated no more than every two years. Non-Immigrant Visa (NIV) demand is difficult to forecast in out-years because the global economy is unpredictable and NIV demand cannot be controlled by CA. The fees were set using a cost model from 2012 and the expenditures were expended in 2014.

- In FY 2017, the Department continued efforts to improve the reliability, accessibility, and standardization of foreign assistance data.
  - Starting with the Bureau of International Narcotics and Law Enforcement Affairs (INL), CGFS and INL worked together to develop and implement the Regional Financial Management System (RFMS) – INL bilateral processing model. This new process accounts and reports all bilateral agreement project funded activity from the project bulk obligation through to expenditures. As part of this upgrade, INL bilateral related procurement transactions automatically integrate the commitment and obligation transactions into RFMS, thereby improving the accuracy of data and eliminating the duplicate entry of thousands of transactions. In addition, INL has established new data structures within the Department's Global Financial Management System that provides new reporting capabilities for tracking and reporting on INL regional program funds by country and project. Building on these new reporting capabilities, CGFS and INL have partnered to implement other reporting improvements leveraging the Global Business Intelligence platform providing the ability to explore, visualize, and report on post-specific INL data.
  - CGFS has also partnered with Office of U.S. Foreign Assistance Resources (F) to implement an extract on foreign assistance spending that corresponds with the data dictionary developed by the Foreign Assistance Data Review working group. This will be a multi-phased effort to provide F, and ultimately the taxpayer via public reporting such as ForeignAssistance.gov, with accurate foreign assistance spending totals, and supporting details on procurements, interagency agreements, grants, and

contributions. The first extract is scheduled for February 2018 for data for the first quarter of FY 2018.

Operating in Contingency and Critical Environments

In some cases, the Department must operate in "critical" environments, or areas that experience various challenges in the form of conflict, instability, disease, or natural disasters. These pose their own set of problems and contribute to existing challenges. The following examples demonstrate ways the Department strives to improve its operations in such environments.

- In response to a recommendation that the Bureau of Near Eastern Affairs (NEA) ensure that they have the appropriate number of certified oversight personnel to oversee Baghdad Life Support Services and Operations (BLiSS contracts), Chief Management Office (CMO) Iraq took several steps to increase contract oversight and to bridge any staffing gaps, including:
    - Alternate Contracting Officer's Representatives (ACORs) are now required to become ACORs for both Operations and Management Support Services (OMSS) and for BLiSS. In this manner, they can provide surge support to each other and assist in staffing any gaps as needed. To ensure the Contracting Officer Representatives (CORs) and ACORs have time to understand the contracts associated with this tertiary responsibility, the CMO and Mission Iraq removed other responsibilities from the COR work requirement statements.
    - Second, the CMO reached out to other Department elements at all sites to ask for subject matter experts to become Government Technical Managers on the contracts. This increases the technical knowledge of the CMO team monitoring each contract without an increase in the number of personnel on the ground at any location.
    - Finally, NEA has approved an additional ACOR for the CMO office, which will provide the CMO with additional depth.
- Prompted by OIG findings in a report on contract management in Kabul, the Department included specific, objective, clear, and measurable performance standards in a statement of work for a new worldwide operations and management contract. The Department awarded a contract that included these standards. The award is an Indefinite Delivery Indefinite Quantity type contract and performance will be accomplished under specific task or requirements-based task orders. The statement of work identifies and includes all known and anticipated operations and maintenance requirements for mission operations.

- Critical Environment Contracting Analytics Staff developed and coordinated 10 risk assessments and 47 contract risk mitigation plans to ensure the safety and security of our Department of State contractor workforce in contingency operation posts and critical environments.

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:

WPEAOmbuds@stateoig.gov