OIG Office of Inspector General

U.S. Department of State • Broadcasting Board of Governors

Fiscal Year 2016 Inspector General Statement On The Department Of State's Major Management And Performance Challenges

OIG-EX-17-01

OUR VISION

To be a world-class organization and a catalyst for effective management, accountability, and positive change in the Department, the Broadcasting Board of Governors, and the foreign affairs community.

OUR MISSION

To conduct independent audits, inspections, evaluations, and investigations to promote economy and efficiency and to prevent and detect waste, fraud, abuse, and mismanagement in the programs and operations of the Department and the Broadcasting Board of Governors.

OUR VALUES

Integrity

We remain independent, striving to maintain the highest level of trust, integrity, and professionalism. Our work is fact-based, objective, and supported by sufficient, appropriate evidence in accordance with professional standards.

Teamwork

Our success depends on working together and fostering an inclusive and mutually supportive environment. Our work environment encourages collaboration, innovation, flexibility, and integration of OIG resources.

Accountability

We accept responsibility for our work products and services, upholding the highest professional standards by evaluating and measuring our results against stated performance measures and targets. We strive to ensure that our work is relevant, credible, and timely.

Communication

We clarify expectations up front and communicate openly, honestly, and accurately with our associates and our stakeholders. We look for ways to improve ourselves and our work products by seeking, giving, and using both praise and constructive feedback.

Respect

We promote diversity and equal opportunity throughout the organization. We value and respect the views of others.

CONTENTS

PROTECTION OF PEOPLE AND FACILITIES

CHALLENGE

Although the Department continues to improve security related training, it lacks consistent implementation of personnel safety standards, and needs to address shortcomings in emergency planning.

The protection of people and facilities overseas remains a significant management challenge for the Department of State (Department). In 2015, personnel and property experienced attacks in Bangladesh, Burundi, Canada, Central African Republic, Iraq, Mali, the Philippines, South Korea, Timor-Leste, Turkey, and Yemen.[1] Incidents included grenade attacks at embassy residences, car bombs detonated in front of consulate facilities, and the non-fatal stabbing of the U.S. Ambassador to South Korea at an official event.[2] Although the Department is committed to protecting its personnel and property (including information), the Office of Inspector General (OIG) continues to find deficiencies related to personnel safety overseas and emergency planning and preparedness.

Personnel Safety Overseas

Given the sensitive nature of OIG's work, many of the reports related to safety and security are classified. However, the information below provides publicly available evidence of the challenges the Department faces in ensuring the safety and security of its people and facilities.
OIG determined that, despite recent improvements, the Department's management and oversight of security personnel is still lacking at posts overseas. Local guard forces failed to perform contractually required duties, such as conducting access control, delivery, and mail screening. If not addressed, these performance deficiencies could allow unauthorized personnel to access the compound or visitors to bring prohibited items into the compound.[3] Failure to investigate and properly and promptly report suspicious or unusual occurrences can delay the reaction time of post officials in an emergency.[4]

Health and safety concerns were also a reoccurring theme in OIG's FY 2016 reports. OIG found deficiencies in seismic risk mitigation in embassy residences[5] and occupational safety and health approvals in overseas housing agreements.[6] OIG also identified life, health, and safety risks to building occupants due to a type of hazardous electrical current known as objectionable current in both the office and apartment complexes at Embassy Kabul.[7] During an audit of the

[1] Department of State, *Bureau of Diplomatic Security Year in Review 2015* (June 2016).

[2] *Ibid.*

[3] OIG, *Audit of Local Guard Force Contractors at Critical- and High-Threat Posts* (AUD-SI-16-33, April 2016).

[4] *Ibid.*

[5] OIG, *Inspection of Embassy Tashkent* (ISP-I-16-12A, March 2016); OIG, *Inspection of Embassy Ashgabat* (ISP-I-16-13A, March 2016).

[6] OIG, *Inspection of Embassy Kinshasa* (ISP-I-16-19A, June 2016).

[7] OIG, *Management Alert: Hazardous Electrical Current in Office and Residential Buildings Presents Life, Health, and Safety Risks at U.S. Embassy Kabul, Afghanistan* (MA-16-01, April 2016).

vehicle-fueling controls and operations and maintenance contract,[8] OIG determined that, in violation of Bureau of Overseas Buildings Operations (OBO) safety standards, the fuel station building had only one exit, located directly above the bulk fuel storage for the fueling station (see figure 1 below). Given the hazardous nature of fuel, if a fire occurred at the fueling station, anyone working in the office building would be at risk.

Figure 1: Fueling Station Office at Embassy Kabul

Source: OIG photo taken at Embassy Kabul on September 9, 2015.

OIG also identified inconsistencies in motor vehicle policies that resulted in a lack of proper training for personnel serving in countries with an elevated risk of car accidents and fatalities.[9] OBO statistics show that of the 773 armored vehicle mishaps that have occurred at overseas posts within the last 5 years, 469 (about 60 percent) were deemed preventable (see figure 2 below). The Department has recognized that driver behavior contributes to vehicle fatalities and that "solutions must center on … providing an effective initial and refresher training program."[10] OIG recommended that the Department establish a mandatory training requirement on armored vehicle safe-driving techniques for all overseas professional chauffeurs and incidental drivers who operate such vehicles.[11]

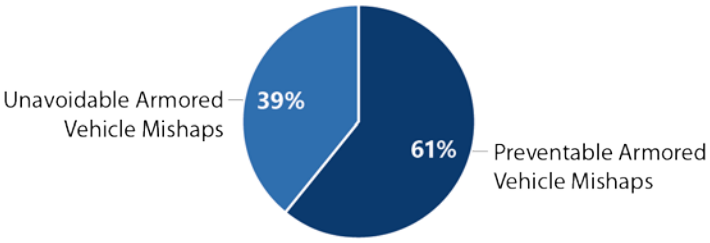
[8] OIG, *Improvements Needed To Strengthen Vehicle-Fueling Controls and Operations and Maintenance Contract at Embassy Kabul, Afghanistan* (AUD-MERO-16-35, April 2016).

[9] OIG, *Inspection of Embassy Ashgabat* (ISP-I-16-13A, March 2016).

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

[11] *Ibid.*

Figure 2: Percentage of Preventable Armored Vehicle Mishaps Overseas



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

Maintaining sufficient physical security at overseas facilities is a fundamental component of protecting U.S. Government employees. Physical security relates to physical measures—such as locked doors, perimeter fences, and other barriers—to protect against unauthorized access (including attackers or intruders) and to safeguard personnel working in those facilities.[12] In recent years, the Department has developed new tools to identify and track physical security deficiencies overseas; however, the Department needs to take additional actions. For example, OIG concluded in a December 2015 report that, until the Department fully implements OIG's recommendations intended to improve the process to request and prioritize physical security needs, it will be unable to identify and address all physical security-related deficiencies. Further, without taking such steps, the Department will be unable to make informed funding decisions based on a comprehensive list of physical security needs.[13]

Emergency Action Planning and Preparedness

When crises arise, planning and preparation can make the difference between life and death. During FY 2016, OIG identified several issues with the Department's emergency action planning and preparedness. For example, in a report published in February 2016, OIG found that chiefs of mission were unaware of the U.S. military assets available during emergency situations.[14] Without this information, embassies and consulates cannot properly plan for emergencies and may be hindered in their responses to actual crises.

OIG also identified shortcomings in the Department's crisis management training and emergency action plans, including at embassies in the Middle East and Africa. OIG found that consular sections in several posts that it inspected in 2016 were unfamiliar with their roles and responsibilities leading up to and during a crisis.[15] Consular managers, faced with competing demands for their time, had not provided sufficient section-wide crisis-specific training to consular staff, thereby increasing vulnerabilities for U.S. citizen security in the event of an

---

[12] 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).

[13] *Ibid.*

[14] OIG, *Inspection of Bureau of Diplomatic Security, Directorate of International Programs* (ISP-I-16-07, February 2016).

[15] OIG, *Inspection of Embassy Kinshasa* (ISP-I-16-19A, June 2016); OIG, *Inspection of Embassy Cairo* (ISP-I-16-15A, April 2016).

emergency.[16] OIG also found that emergency action plans were out of date, lacked key information, included erroneous points of contact, or were improperly certified by leadership.[17] Without adequate staff training and a properly documented and tested emergency action plan, embassies and consulates cannot effectively mitigate the risks that a disaster or unforeseen incident poses to its operations.

Recent Department Actions to Address the Protection of People and Facilities

Personnel Safety Overseas

- The Department expanded its Foreign Affairs Counter-Threat training, a program in which diplomats learn defensive driving, how to recognize an improvised explosive device, firearms familiarization, tactical medical skills, and surveillance detection. This training is currently required for Department personnel assigned to two dozen posts where the threat is highest. The Department is considering requiring universal training for all overseas staff.[18]
- The Department completed seismic hazard ratings for residences at affected posts and, for residences rated poor, is in the process of identifying alternative residences that meet acceptable seismic ratings.[19]
- As a result of OIG's management assistance report on armored vehicles, the Department is in the process of identifying all drivers of armored vehicles and developing a budget request to fund motor vehicle training for those drivers.[20]

Emergency Planning and Preparedness

- In response to OIG's inspection of the Bureau of Diplomatic Security, Directorate of International Programs, the Department conducted a webinar on coordinating with the Department of Defense's Military Crisis Response Force and issued a Department-wide cable that addressed Department and interagency support of embassy security.[21]
- In response to OIG inspection recommendations, the Department is updating emergency action plans and has updated consular emergency preparedness documents, processes and training for numerous overseas missions.[22]

---

[16] OIG, *Inspection of Embassy Kinshasa* (ISP-I-16-19A, June 2016).

[17] OIG, *Inspection of Embassy Cairo* (ISP-I-16-15A, April 2016); OIG, *Inspection of Embassy Kinshasa* (ISP-I-16-19A, June 2016); OIG, *Inspection of Bureau of Energy Resources* (ISP-I-16-06, February 2016).

[18] Department of State, *Bureau of Diplomatic Security Year in Review 2015* (June 2016).

[19] OIG, *Inspection of Embassy Tashkent* (ISP-I-16-12A, March 2016); OIG, *Inspection of Embassy Ashgabat* (ISP-I-16-13A, March 2016).

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

[21] OIG, *Inspection of the Bureau of Diplomatic Security, Directorate of International Programs* (ISP-I-16-07, February 2016).

[22] OIG, *Inspection of Embassy Cairo* (ISP-I-16-15A, April 2016); OIG, *Inspection of Embassy Kinshasa* (ISP-I-16-19A, June 2016); OIG, *Inspection of Bureau of Energy Resources* (ISP-I-16-06, February 2016).

MANAGING POSTS AND PROGRAMS IN CONFLICT AREAS

CHALLENGE

The Department continues to face significant challenges managing posts and programs in conflict areas, including areas affected by overseas contingency operations.

In addition to the overall challenge of protecting its people and facilities, the Department faces a much more specific challenge in managing its posts and programs that are located in conflict areas. This challenge is particularly pronounced in areas affected by overseas contingency operations. Missions in countries such as Iraq, Afghanistan, and Pakistan are at the forefront of U.S. engagement to counter terrorism, stabilize fragile states, and respond to regional conflicts. The Department's FY 2017 congressional budget justification requested $14.9 billion in overseas contingency operations funds to address a number of continuing and emerging challenges, including response to the crisis in Syria, efforts to counter the Islamic State in Iraq and the Levant (ISIL), and operations in Afghanistan and Pakistan.

Conflict areas are typically marked by violence, humanitarian crises, political instability, physical insecurity, weak governance, and rampant corruption. As a result, programs and posts operating in these areas must adapt to constant change, pervasive security concerns, dramatic swings in personnel and funding, and widespread reliance on contractors and grantees. Recognizing the particular difficulties of managing posts and programs in conflict areas as well as the fact that the Department has invested billions of dollars to do so, OIG continues to focus closely on the complex issues affecting Department operations in unstable environments.

Post Infrastructure and Logistical Support

The turbulent conditions in and around conflict areas, frequently coupled with an influx of personnel and increased demand for resources, continue to present management obstacles for the Department. These problems include recurring difficulties in managing fuel storage and control at posts in conflict areas. Reiterating concerns first raised in 2010,[23] OIG identified during this reporting period inventory control and safety deficiencies in fuel storage and refueling operations at Embassy Kabul.[24] Posts in conflict areas also struggle to keep pace with construction and maintenance demands for facilities and infrastructure. OIG issued a Management Assistance Report in April 2016 to alert the Department to a potential safety risk that could result in severe injury or death involving electrical current; this issue was identified by the U.S. Army Corps of Engineers during the course of an ongoing audit of construction of the new office and residential apartment buildings at Embassy Kabul.[25] OIG's findings and

[23] OIG, *PAE Operations and Maintenance Support at Embassy Kabul, Afghanistan Performance Evaluation* (MERO-I-11-05, December 2010).

[24] OIG, *Improvements Needed To Strengthen Vehicle-Fueling Controls and Operations and Maintenance Contract at Embassy Kabul, Afghanistan* (AUD-MERO-16-35, April 2016).

[25] OIG, *Management Alert: Hazardous Electrical Current in Office and Residential Buildings Presents Life, Health, and Safety Risks at U.S. Embassy Kabul, Afghanistan* (MA-16-01, April 2016).

recommendations regarding construction of these new facilities will not be finalized until later in FY 2017, but OIG notified the Department of the current concern so that it could immediately evaluate and address this potential risk. Finally, as described in more detail below, because the Department and other agencies lack the organic capacity to meet the increased demands of overseas contingency operations and other operations in conflict areas, most logistical support is provided by contractors. This adds unique contract management challenges to other issues that are already posed by conflict areas.

Managing Contracts, Grants, and Cooperative Agreements in Conflict Areas

Conflict areas present unique obstacles to effective management of contracts and grants that go beyond those identified in the separate management challenge discussed subsequently. Although the problems that occur in conflict areas are often substantively similar to those that occur elsewhere, the ramifications of those problems may be amplified because of stresses particular to conflict areas (for example, the quick turnover of government personnel or the increased cost of operations). In recent years, the Department has focused efforts on improving management of contracts, grants, and cooperative agreements in these areas, but heavy reliance on contractors and grantees remains a necessity in conflict areas, and OIG continues to find instances of insufficient oversight. We include examples of these issues below.

OIG inspected the Bureau of Diplomatic Security's (DS) Directorate of International Programs, which is responsible for the oversight of more than $1.6 billion in 90 local guard contracts around the world (including conflict areas), approximately 80 personal services agreements for local guard forces, and 8 task orders for the Worldwide Protective Services contract that provides security for Embassy Baghdad and consulates throughout Iraq. OIG found that the Department's efforts to provide DS with contract administration assistance were hampered by the lack of service-level agreements and uniform operating procedures. This led to misunderstandings about staff roles and responsibilities.[26]

Audits of contracts in Iraq revealed over $20 million in questioned and unsupported costs and unallowable fees. An audit of task orders awarded under the Operations and Maintenance Support Services contract found that Department officials did not prepare comprehensive planning documents, formally assign oversight personnel, or ensure that oversight personnel adequately documented the contractor's performance. As a result, the Department had no basis or justification to hold the contractor accountable for identified weak performance. In addition, the Department did not comply with statutory and Department requirements for timely agreement on contract terms, specifications, and the price of the task orders, resulting in the contractor being paid more than $500,000 in unallowable fees.[27]

In an audit of the Baghdad Life Support Services contract, OIG found that the Department acted contrary to the Federal Acquisitions Regulations (FAR) by awarding four task orders that

[26] OIG, *Inspection of the Bureau of Diplomatic Security, Directorate of International Programs* (ISP-I-16-07, February 2016).

[27] OIG, *Audit of Task Orders for the Union III Compound Awarded Under the Operations and Maintenance Support Services Contract* (AUD-MERO-16-41, July 2016).

provided overtime or incentive pay to contractors whose labor costs were established as firm-fixed-price in the contract. The Department's decision to award these task orders was not accompanied by a cost-benefit analysis, validated need, or written justification. As a result, OIG found that the Department paid the contractor $184,400 for overtime that was contrary to the FAR and questioned $2.8 million paid to the contractor in incentive fees without a documented benefit for the Department.[28]

Audits of security services contracts for Embassy Baghdad and Consulate Erbil identified insufficient review of supporting documentation for contractor invoices by contracting officer's representatives (CORs), leading to over $17 million in questioned and unsupported costs.[29]

OIG's inspection of the Bureau of Democracy, Human Rights, and Labor (DRL) programs in Iraq also noted the challenges the Department faces in managing grants in this environment. All 12 grants that were active between October and November 2015 (with a total award value of more than $42 million) had the necessary monitoring plans, performance indicators, and risk assessment or contingency plans.[30] However, given security restrictions, neither DRL employees nor Embassy Baghdad employees had conducted site visits to Iraq grant recipients since 2013. Instead, DRL relied on local contractors to visit grant recipient sites.

Section 846 of the National Defense Authorization Act for Fiscal Year 2013 requires the Department to conduct comprehensive risk assessments whenever contractors are involved in supporting overseas contingency operations. For those high-risk areas that are identified, the Department must prepare risk mitigation plans. OIG reviewed the Department's risk assessment for Afghanistan and Iraq and found that the Department had not prepared plans for 14 of 32 areas in Afghanistan and 32 of 52 in Iraq. OIG was particularly concerned with the absence of mitigating action plans for high-risk areas concerning oversight of contractor operations. This is an issue that OIG has addressed repeatedly; in the last 2 years, OIG has issued four other reports[31] identifying problems related to the high-risk areas of insufficient program managers, contracting officers, CORs, and acquisition workforce personnel.[32]

2016 audits and inspections also highlighted issues with contractors performing inherently government functions. In Afghanistan, OIG found that contractors were accepting fuel delivered

---

[28] OIG, *Management Assistance Report: Improper Use of Overtime and Incentive Fees under the Department of State Baghdad Life Support Services (BLiSS) Contract* (AUD-MERO-16-08, November 2015).

[29] OIG, *Audit of Bureau of Diplomatic Security Worldwide Protective Services Contract Task Order 3— Baghdad Embassy Security Force* (AUD-MERO-16-28, February 2016); OIG, *Audit of Bureau of Diplomatic Security Worldwide Protective Services Contract Task Order 8 – Security Services at U.S. Consulate Erbil* (AUD-MERO-16-30, March 2016).

[30] OIG, *Evaluation of Bureau of Democracy, Human Rights, and Labor Iraq Programs in Support of Line of Effort 1 of the President's Counter-ISIL Strategy* (ISP-16-09, March 2016).

[31] OIG, *Audit of the Bureau of Diplomatic Security Worldwide Protective Services Contract Task Order 3—Baghdad Embassy Security Force* (AUD-MERO-16-28, February 2016); *OIG, Audit of the Bureau of International Narcotics and Law Enforcement Affairs Aviation Support Services Contract in Iraq* (AUD-MERO-15-35, July 2015); OIG, *Audit of the U.S. Mission Iraq Medical Services Contract* (AUD-MERO-15-25, May 2015); *OIG, Audit of Vehicle-Fueling Controls and Operations and Maintenance Contract at Embassy Kabul, Afghanistan* (AUD-MERO-16-35, April 2016).

[32] OIG, *Additional Actions Are Needed To Fully Comply With Section 846 of the National Defense Authorization Act for Fiscal Year 2013 Concerning Critical Environment Contracting* (AUD-MERO-16-50, September 2016).

on behalf of the embassy and thus effectively authorizing payment, which is an inherently governmental function and contrary to the Department's Foreign Affairs Manual (FAM) regulations. In Iraq, contractors were serving as grants officer's representatives for one-third (4 out of 12) of the active grants.[33]

As a result of a complaint referred by the Government Accountability Office (GAO) alleging mismanagement, OIG conducted a review of the Department's cooperative agreement with Southern Methodist University to support the enhancement of the Department of Psychology at a university in Peshawar. OIG found that the embassy had not properly monitored the award because security concerns prevented Embassy Islamabad's Public Affairs Section from making required site visits. In addition, one of the objectives had not been completed, and materials and equipment purchased in January 2014 remained unused. The Department deobligated more than $300,000 and focused attention on meeting the agreed-upon objectives.

During an inspection of Embassy Ankara, OIG found that the CORs' files in Embassy Ankara and Consulate Adana were incomplete. The Department's failure to provide adequate contract oversight constitutes a risk for monitoring and documenting the contractor's technical progress and expenditures of resources.[34]

The Department faces unique difficulties in branding U.S.-sponsored events in environments with complex and rapidly changing security situations. The right balance between reasonable caution and the need to identify American-sponsored events must be found. Embassy public affairs sections often handle branding event-by-event, rather than having an overall strategy and process that has been reviewed by a panel of experts. In one example of this issue, OIG recently recommended that the Department implement a policy for consistent branding of U.S.-sponsored public events in Egypt.[35] Striking the right balance is difficult, but failing to do so could hamper opportunities to build relationships with target audiences or, conversely, potentially put the lives of embassy staff at risk.

Coordination of Programs

OIG and other offices of inspectors general have found that coordination has been a critical shortfall in U.S. programs and activities in previous overseas contingency operations, and interagency and intra-agency coordination remain a challenge in conflict areas.

A 2016 OIG inspection of Embassy Baghdad's implementation of Line of Effort 6 in the President's comprehensive strategy to defeat ISIL found that the post's public diplomacy activities were not fully integrated with the government-wide effort to "expose ISIL's true

---

[33] OIG, *Improvements Needed To Strengthen Vehicle-Fueling Controls and Operations and Maintenance Contract at Embassy Kabul, Afghanistan* (AUD-MERO-16-35, April 2016); OIG, *Evaluation of Bureau of Democracy, Human Rights, and Labor Iraq Programs in Support of Line of Effort 1 of the President's Counter-ISIL Strategy* (ISP-16-09, March 2016).

[34] OIG, *Inspection of Embassy Ankara, Turkey* (ISP-I-16-24A, September 2016).

[35] OIG, *Inspection of Embassy Cairo* (ISP-I-16-15A, April 2016).

nature" and also operated without formal post-level strategic planning or goals.[36] The Department and its interagency partners have made recent changes to improve government-wide implementation of Line of Effort 6 and countering violent extremism efforts in general. The White House established the Global Engagement Center within the Department on March 14, 2016, to coordinate U.S. counterterrorism messaging to foreign audiences.[37]

OIG found a lack of coordination of foreign assistance efforts during its inspection of Embassy Cairo. The Department had funded a program in Egypt without the Ambassador's written approval and several sections and agencies at the embassy were generally unaware of a standard procedure for obtaining written Chief of Mission approval. Such procedures are necessary to avoid duplication, waste, lack of support to integrated country strategy goals, unintended effects on the bilateral relationship, and imposition of a monitoring burden the Embassy cannot meet.[38]

Recent Department Actions to Address Management of Posts and Programs in Conflict Areas

- The Department published a policy on "Critical Environment Contracting" and created an office, the Critical Environment Contracting Analytics Staff, with responsibility for developing, coordinating, and implementing the risk assessments and mitigation plans for critical environment contracts.[39]
- The White House established the Global Engagement Center within the Department to coordinate U.S. counterterrorism messaging to foreign audiences.
- The Department implemented an innovative model for diplomacy and program management via the Syria Transition Assistance and Response Team in Turkey.
- In response to an OIG audit, the Bureau of Near Eastern Affairs (NEA), Office of Assistance Coordination has updated its Management Policies and Procedures Manual, in compliance with regulations to enable NEA to obtain reasonable assurance that award recipients have adequate financial management controls in place.[40]
- The Bureau of African Affairs established and implemented policies and procedures to provide guidance to bureau personnel serving as CORs for all contract-related responsibilities, including pre-award activities, contract administration, maintaining files, and closing out contracts. These procedures require program offices to review COR files and activities at least biannually.[41]

---

[36] OIG, *Evaluation of Embassy Baghdad's Implementation of Line of Effort 6 in the President's Strategy to Counter ISIL: Exposing ISIL's True Nature* (ISP-I-16-10, March 2016).

[37] Executive Order 13721, "Developing an Integrated Global Engagement Center To Support Government-wide Counterterrorism Communications Activities Directed Abroad and Revoking Executive Order 13584" (March 14, 2016).

[38] OIG, *Inspection of Embassy Cairo* (ISP-I-16-15A, April 2016).

[39] 14 FAM 240.

[40] OIG, *Audit of the Bureau of Near Eastern Affairs Financial Management of Grants and Cooperative Agreements Supporting the Middle East Partnership Initiative* (AUD-MERO-16-42, July 2016).

[41] OIG, *Compliance — Audit of the Administration and Oversight of Contracts and Grants Within the Bureau of African Affairs (*AUD-CG-14-31, May 26, 2016).

- After the 2012 attack in Libya, DS and the U.S. Marine Corps accelerated the activation of new security guard detachments at 21 posts around the world including Beirut, Lebanon; Erbil, Iraq; and Lahore, Pakistan. As of October 2015, 14 more new detachments were being planned, and the Department had increased the number of Marines in 143 existing detachments.[42]
- The Department has developed a course called "Diplomacy at High Threat Posts." The course identifies best practices for effective work in high-threat/high-risk environments and strategies for close collaboration among heads of agencies at post.

[42] Department of State, *Bureau of Diplomatic Security Year in Review 2015* (June 2016).

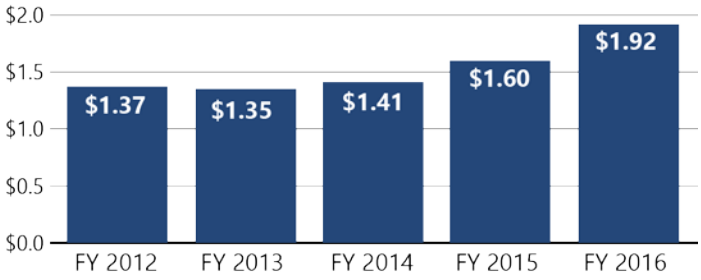
INFORMATION SECURITY AND MANAGEMENT

CHALLENGE

The Department needs to adequately protect its information systems and electronic data from internal and external threats, consistently implement a 21st century records management program, and effectively coordinate the acquisition and management of its high-value IT investments.

The Department depends on information systems and electronic data to carry out essential mission-related functions. The security of these systems and networks is vital to protecting national and economic security, public safety, and the flow of commerce.[43] These information systems are subject to serious threats that can have adverse effects on organizational operations, assets, individuals, and the nation; in particular, these effects include exploiting both known and unknown vulnerabilities to compromise the information being processed, stored, and transmitted by those systems. The Department has spent several billion dollars in the past 5 years (see figure 3 below) on software tools, IT equipment, and professional expertise. However, given the complexity and sensitivity of the Department's IT apparatus and the numerous security breaches it has suffered in recent years, IT security and management continues to be a significant management challenge.

Figure 3: Department of State IT Spending
($ Billions)



Source: Office of Management and Budget, Department of State's Information Technology Agency Summary (September 2016).

Cybersecurity

The U.S. Government's global computer networks are tempting targets for hackers, spies, and other intruders.[44] Since the majority of Department communications and operations rely heavily on computer systems, cyberattacks pose a serious threat to the protection of information. The 2014 intrusion into the Department's network, for example, highlighted the importance of being prepared to restore operations promptly while protecting information and the systems that

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

[44] Department of State, *Bureau of Diplomatic Security Year in Review 2015* (June 2016).

process it.[45] In FY 2016, OIG reported significant weaknesses in the Department's cybersecurity incident response and reporting program.[46] The Department's efforts to respond to incidents (including denial-of-service, malicious code, and unauthorized access) showed that it had not complied with its own information security policies in more than 55 percent of the incidents that OIG reviewed.

In FY 2016, OIG found network user account management to be another cybersecurity vulnerability. In its management assistance report on the Department's Active Directory (AD), OIG determined that 74 percent of more than 2,500 inactive accounts were inactive for more than 1 year, and the remaining accounts were inactive for greater than 90 days.[47] This occurred, in part, because the Department does not have a centralized process for AD account management. If an unneeded account remains active, an intruder could gain access to the account, elevate or change its access permissions, and gain access to sensitive information that could compromise the integrity of the Department's network and cause widespread damage across the Department's IT infrastructure. Moreover, if an intruder gains access to an inactive account with elevated or administrative privileges, the intruder could access personally identifiable information without being detected, creating the risk of data loss and theft and compromising user identities and the accountability of user actions.

The lack of a properly developed and tested IT contingency plan that is linked with overall emergency preparedness processes could be detrimental to a post's or bureau's recovery efforts following an unforeseen incident. In its February 2016 management assistance report on this issue, OIG continued to find deficiencies in Department IT contingency planning at overseas posts, despite a December 2011 OIG memorandum to the Bureau of Information Resources and Management (IRM) that stated that bureau and post emergency preparedness activities had not devoted sufficient attention to the development and testing of IT contingency plans.[48] OIG identified a lack of IT contingency planning in 69 percent (20 out of 29) of overseas inspections performed during FYs 2014 and 2015.[49]

Additionally, OIG found that the Department's Chief Information Officer (CIO), who is the head of IRM, is not properly positioned to ensure that the Department's information security program is effective. Under the Department's current organizational reporting structure, the CIO reports to the Under Secretary for Management. DS reports separately to the Under Secretary for Management. According to Department guidance, IRM and DS both have statutory responsibilities for information security. Under this reporting structure, DS and any other bureau

---

[45] OIG, *Semiannual Report to Congress* (October 1, 2015–March 31, 2016).

[46] OIG, *Management Assistance Report: Department of State Incident Response and Reporting Program* (AUD-IT-16-26, February 2016).

[47] OIG, *Management Assistance Report: Inactive Accounts Within the Department of State's Active Directory* (AUD-IT-16-37, June 2016).

[48] OIG, *Management Assistance Report: Continued Deficiencies Identified in Information Technology Contingency* Planning (ISP-I-16-05, February 2016); OIG, *Inspection of Embassy Cairo* (ISP-I-16-15A, April 2016); OIG, *Inspection of Embassy Ashgabat* (ISP-I-16-13A, March 2016).

[49] OIG, *Management Assistance Report: Continued Deficiencies Identified in Information Technology Contingency Planning* (ISP-I-16-05, February 2016).

or office reporting to the Under Secretary for Management are not required to communicate information security risks to IRM. Further, bureaus could miscommunicate information security risks to leadership, which in turn could increase the likelihood and impact of potential attacks. Without a centralized reporting structure, bureaus may accept risks associated with one mission or business function without understanding the potential effect on the Department as a whole.[50]

Electronic Records Management

For the last two decades, both Department policy and Federal regulations have explicitly stated that emails may qualify as Federal records. As is the case throughout the Federal Government, management weaknesses at the Department have contributed to the loss or removal of email records, particularly records created by the Office of the Secretary. These weaknesses include a limited ability to retrieve email records, inaccessibility of electronic files, failure to comply with requirements for departing employees, and a general lack of oversight.[51] In FY 2016 OIG identified records management deficiencies at many levels of the Department. In addition to issues in the Office of the Secretary, two domestic bureaus were found to have noncompliant records management programs, and several posts overseas inconsistently employed the Department's official record email tool,[52] thereby increasing the risk of a loss of institutional knowledge and potentially creating an inability to locate and retrieve documents or communications necessary to support key operations.[53]

During its review of issues associated with records preservation and the use of personal hardware and software by five Secretaries of State, OIG determined that email usage and preservation practices varied across the tenures of the five most recent Secretaries and that compliance with statutory, regulatory, and internal requirements varied as well.[54] OIG recommended that the Department enhance and more frequently issue guidance on the permissible use of personal email accounts to conduct official business, amend policies to provide for administrative penalties for failure to comply with records preservation and cyber security requirements, and develop a quality assurance plan to address vulnerabilities in records management and preservation.[55]

OIG also determined that Department leadership had not played a meaningful role in overseeing or reviewing the quality of responses to Freedom of Information Act (FOIA) requests for records involving the Office of the Secretary. OIG's 2016 evaluation of the Department's FOIA

---

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

[51] OIG, *Office of the Secretary: Evaluation of Email Records Management and Cybersecurity Requirements* (ESP-16-03, May 2016).

[52] OIG, *Inspection of Embassy Tashkent* (ISP-I-16-12A, March 2016); OIG, *Inspection of Embassy Cairo* (ISP-I-16-15A, April 2016); OIG, *Inspection of Embassy Tegucigalpa* (ISP-I-16-21A, August 2016); OIG, *Inspection of Kinshasa* (ISP-I-16-19A, June 2016).

[53] OIG, *Inspection of the Bureau of International Organization Affairs* (ISP-I-16-02, October 2015); OIG, *Inspection of the Bureau of Energy Resources* (ISP-I-16-06, February 2016).

[54] OIG, *Office of the Secretary: Evaluation of Email Records Management and Cybersecurity Requirements* (ESP-16-03, May 2016).

[55] *Ibid.*

processes found that searches performed by the Office of the Secretary did not consistently meet statutory and regulatory requirements for completeness, rarely met requirements for timeliness, and were occasionally found to be inaccurate.[56] According to OIG's evaluation, procedural weaknesses in the Department's FOIA processes, such as a lack of management oversight, an absence of written policies and procedures, and a lack of training, appeared to contribute to these deficiencies.

IT Investment Planning and Management

IT investments can have a dramatic effect on an organization's performance. Well-managed IT investments that are selected carefully and focus on meeting mission needs can propel an organization forward, dramatically improving performance while reducing costs.[57] Likewise, poor investments that are inadequately justified or have poorly managed costs, risks, and expected mission benefits can hamper an organization's performance.[58]

Although the Government spends significant funds on IT activities ($380 billion between FY 2011–2015),[59] GAO reported that, since 2000, the Federal Government has achieved little of the productivity improvements that private industry has realized from IT.[60] As noted in the 2015 GAO High-Risk Series Update,[61] "federal IT investments too frequently fail to be completed or incur cost overruns and schedule slippages while contributing little to mission-related outcomes." OIG's work has confirmed that the Department experiences many of the same problems.

In FY 2016, OIG reported on the Department's process for selecting and approving IT investments and found that the Department did not require bureaus to assess the potential duplication of planned IT acquisitions.[62] Also, the Department generally did not select IT investments in accordance with the process it had designed or with Office of Management and Budget (OMB) requirements, resulting in duplicative IT investments and a lack of visibility into the Department's IT portfolio.

OIG also reported that the Department did not always report to OMB accurate and complete information on its IT investments. This occurred primarily because the process to prepare the reports is manual and involves numerous users across the Department; insufficient IRM oversight of the reporting process further exacerbated the problem. Because some of the

---

[56] OIG, *Evaluation of the Department of State's FOIA Processes for Requests Involving the Office of the Secretary* (ESP-16-01, January 2016).

[57] OIG, *Audit of the Department of State Process To Select and Approve Information Technology Investments* (AUD-FM-16-31, March 2016).

[58] GAO, *Assessing Risks and Returns: A Guide for Evaluating Federal Agencies' IT Investment Decision-making* (GAO/AIMD-10.1.13, February 1997).

[59] OMB, *Department of State's Information Technology Agency Summary* (ITDASHBOARD.GOV, September 2016).

[60] GAO, *Leveraging Best Practices and Reform Initiatives Can Help Agencies Better Manage* Investments (GAO-14-568T, May 2014).

[61] GAO, *Report to Congressional Committees, High Risk Series, An Update* (GAO-15-290, February 2015).

[62] OIG, *Audit of the Department of State Process To Select and Approve Information Technology Investments* (AUD-FM-16-31, March 2016).

reports were inaccurate and incomplete, Department stakeholders, such as OMB and Congress, had limited ability to analyze and assess IT spending.[63]

As in prior years, OIG's annual assessment of the Department's Information Security Program identified numerous control weaknesses that significantly affected program effectiveness, and increased the Department's vulnerability to cyberattacks and threats.[64] Since 2010, OIG has reported that the Department lacks effective risk management for all phases of the system development lifecycle.[65] These problems, however, have persisted. For example, in the October 2015 inspection of IRM's Vendor Management Office (VMO), OIG found a lack of consistent implementation of iSchedule, a system that provides the framework for integrating IT project schedules to enable IRM to assign and manage work, monitor and control progress toward milestones, and understand the relationships and dependencies among IT projects. This inconsistent use of iSchedule results in inadequate bureau coordination and incomplete project data and limits visibility on projects, activities, and risk.

Recent Department Actions to Address Deficiencies Related to IT

Cyber Security

- DS offices collaborated to provide cyber threat analysis to regional security officers, thereby providing diplomatic posts with tools that are intended to enable them to address such threats directly.[66]
- The DS cyber team launched technical, managerial, and operational security responses overseen by an interagency task force made up of DS, the National Security Agency, the Department of Homeland Security, and industry experts. The Department emerged with a new capacity to stop suspicious emails and identify malicious attachments that are designed to evade traditional security defenses. [67]
- As a result of the Department's distribution of cybersecurity threat information and best practices, 102,000 network users have completed Cybersecurity Awareness training, and more than 33,000 users visited the website for information on social media, mobile devices, and spear phishing. DS delivered 379 cyber threat briefings to 7,700 overseas personnel. [68]

[63] *Ibid*.

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

[65] OIG, *Inspection of the Bureau of Information Resource Management, Operations, Vendor Management Office* (ISP-I-16-03, October 2015).

[66] Department of State, *Bureau of Diplomatic Security Year in Review 2015* (June 2016).

[67] *Ibid.*

[68] *Ibid.*

Records Management

- The Department initiated a program, approved by the National Archives and Records Administration (NARA), to archive all of the email of certain senior officials.[69]
- The Department has requested additional resources in FY 2017 to help address its historically underfunded FOIA program.[70]
- The Department hired a Transparency Coordinator tasked with leading its efforts to meet the President's Managing Government Records Directive, responding to OIG's recommendations, and working with other agencies and the private sector to explore best practices and new technologies.
- The Department is in the process of selecting new technology, which will assist in meeting the deadlines that have been set both by the White House and NARA for managing email records electronically. The Department hopes to have that new technology in place by the end of calendar year 2016, which will greatly enhance records-keeping and FOIA capability. [71]
- The Department initiated a program, approved by the NARA, to archive all of the email of certain senior officials.[72]

IT Investment Planning and Management

- IRM designed a process to support the selection and approval of major and non-major IT investments that addresses the majority of key OMB requirements.[73]
- IRM designed a tool, iMatrix, to assist in managing the Department's IT capital planning process. iMatrix facilitates IT project management and the reporting of IT investments. Key requirements from OMB's IT investment requirements were built into the application. For example, iMatrix includes a section where bureaus and offices can document their analysis of alternatives. The iMatrix application can retain all required documentation related to the selection, control, and evaluation of each IT investment.[74]

---

[69] Department of State, *Briefing on the Inspector General Report, Office of the Secretary: Evaluation of Email Records Management and Cybersecurity Requirements* (Senior State Department Officials via Teleconference, May 2016), http://www.state.gov/r/pa/prs/ps/2016/05/257733.htm).

[70] *Ibid.*

[71] *Ibid.*

[72] *Ibid.*

[73] OIG, *Audit of the Department of State Process To Select and Approve Information Technology Investments* (AUD-FM-16-31, March 2016).

[74] *Ibid.*

OVERSIGHT OF CONTRACTS AND GRANTS

CHALLENGE

The Department needs to fully address the proper management, oversight, and accountability of contracts and procurements, including grants and cooperative and interagency agreements.

For FY 2016, the Department spent substantial resources on contracts, grants, and cooperative agreements. This same year, OIG issued four management assistance reports addressing the Department oversight of contracts and grants, and OIG's Office of Investigations opened 31 cases related to contract and procurement fraud. As the Department engages in increasingly complex acquisitions to procure needed services and supplies and awards grants to support U.S. foreign policy goals, the Department continues to face challenges in the proper management, oversight, and accountability of these instruments around the globe. The Department needs to ensure that contractors and grantees are properly chosen, work is properly conducted and monitored, objectives are achieved, and costs are effectively contained.

Award Management

OIG continues to identify issues with effective management of high-value, critical contracts. In several reviews, inspectors and auditors noted that routine contract management tasks such as validating performance metrics to assess contractor performance, maintaining complete and accurate procurement files, conducting proper invoice review, and modifying contracts, did not comply with guidance set forth in the FAR, the Foreign Affairs Handbook (FAH), and the FAM.

An OIG inspection of IRM's VMO found that the office operated without authority to require compliance with its procedures and that, at times, it was accordingly difficult for the office to compel some of the CORs and government technical monitors (GTMs) to follow its procedures and processes. The inspection and a subsequent audit also concluded that the processes used by IRM employees to calculate and validate contractor qualifications and the amount of performance incentive payments were inconsistent, time consuming, and manual.[75] These inconsistent reviews by GTMs resulted in the Department paying performance incentive fees to Vanguard contractors without complete validation of their performance metrics.[76] The VMO also performed some contract administration duties for the $3.5 billion Vanguard acquisition without formal delegation from the contracting officer or an adequate document retention policy.

OIG identified several lapses in internal contract management controls. Inspectors in Cairo found that the embassy did not prepare an annual acquisition plan, neglecting to incorporate market research to identify the best contract method for competition and possible cost savings. In

[75] OIG, *Audit of Time and Material Expenses and Performance Incentive Payments under the Bureau of Information Resource Management, Vendor Management Office Vanguard Program* (AUD-CGI-16-34, May 2016).

[76] OIG, *Inspection of the Bureau of Information Resource, Management, Operations, Vendor Management Office* (ISP-I-16-03, October 2015).

addition, embassy procurement files did not comply with Federal regulations requiring documentation of sole source justifications.[77] Management lapses also significantly contributed to incidents of contract fraud at several posts overseas. A joint investigation by OIG and DS uncovered a large-scale theft of approximately $2.3 million in diesel fuel from Embassy Tbilisi. Following another investigation in FY 2016, OIG recommended that, rather than simply documenting how fraud was conducted, the Department should focus on the internal control breaches that allowed fraud to continue.[78]

In addition to the instances noted above, grants management also remains a challenge for the Department. In FY 2016 OIG published 9 reports concerning grants and included 14 formal recommendations to improve monitoring, reporting, documentation, and overall grants coordination.

Monitoring of Grantee Performance and Financial Management

Monitoring is a key component of performance management. It helps measure progress against goals and indicators of performance, reveals whether desired results are occurring, and confirms whether implementation is on track.[79] Financial monitoring should include site visits to review recipients' financial policies and procedures, financial management controls, and supporting documentation.[80] OIG audits and inspections of Department grants identified the need for improved management and monitoring of grantees.

For example, during its inspection of Embassy Tashkent, OIG found that the embassy did not document its risk management actions on grants it awarded, did not create performance monitoring plans, and did not document grant performance reporting. Failure to assess and document risk during the award period leaves the U.S. Government vulnerable to loss of funds, grantee fraud, or grantee failure to perform; failure to develop and carry out a monitoring plan prevents the mission from verifying that the grant objective is being carried out in the interest of the U.S. Government and that taxpayer dollars are well-spent.[81] Similarly, OIG inspectors found that embassies Ashgabat and Tegucigalpa did not have performance monitoring plans or did not document performance for all grants. In Embassy Ashgabat, the grants officer and grants officer representatives told OIG that the embassy monitored grantee performance but did not document that monitoring.[82] An audit of the financial management grants and cooperative agreements supporting the Middle East Partnership Initiative found that the NEA's grant monitoring process was not designed to prevent or detect unallowable or unsupported costs. In a final example, an audit of the Bureau of Political-Military Affairs found that the lack of grantee

[77] OIG, *Inspection of Embassy Cairo* (ISP-I-16-15A, April 2016).

[78] OIG, *Inspection of Embassy Kinshasa* (ISP-I-16-19A, June 2016).

[79] Department of State, *Evaluation Policy*, January, 2015.

[80] OMB, *Circular A-110*, Subpart C, Section 21 (b)(1) and (3).

[81] OIG, *Inspection of Embassy Tashkent* (ISP-I-16-12A, March 2016).

[82] OIG, *Inspection of Embassy Ashgabat* (ISP-I-16-13A, March 2016).

oversight made it difficult for the Bureau to ensure that award recipients were using funds to support its overall mission and programs.[83]

Recent Department Actions to Address Deficiencies Related to Oversight of Contracts and Grants

- In response to recommendations from OIG's 2015 inspection, Embassy Cairo developed an annual acquisition plan.[84]
- In response to OIG inspections in 2015 and 2016, the Department is in the process of establishing management and monitoring procedures of grantees for embassies Tashkent, Ashgabat, and Cairo.[85]
- In response to OIG inspections in 2015 and 2016, the Department prepared a Federal Assistance Human Capital Plan to ensure that it had acquired the appropriate number of trained personnel to properly conduct grants management and monitoring procedures of grantees at embassies Tashkent, Ashgabat, and Cairo.[86]
- The Department is in the process of establishing a service level agreement between DS and the Bureau of Administration to address the Bureau of Administration's oversight of DS's overseas protective services contractors worth more than $1.6 billion. In response to OIG recommendations, DS is in the process of implementing standard operating procedures for CORs, contracting officers, and specialists. [87]
- The Office of the Procurement Executive conducted a grants management review of Bureau of African Affairs (AF). As a result, AF created a standard operating procedure for Federal assistance management. AF specialists are also holding numerous grants management training sessions for Bureau posts via digital video conferencing, telephone conferencing, and live training sessions.[88]
- The Department is in the process of providing guidance to CORs and GTMs on performing assigned duties.[89]
- The Department deployed a new database to facilitate more efficient and timely reporting of the Vanguard contractor's performance metrics. [90]

---

[83] OIG, *Audit of the Bureau of Political-Military Affairs Federal Assistance Awards* (AUD-SI-16-49, September 2016).

[84] OIG, *Inspection of Embassy Cairo* (ISP-I-16-15A, April 2016).

[85] OIG, *Inspection of Embassy Tashkent (*ISP-I-16-12A, April 2016); OIG, *Inspection of Embassy Ashgabat* (ISP-I-16-13A, April 2016); OIG, *Inspection of Embassy Cairo* (ISP-I-16-15A, April 2016).

[86] *Ibid.*

[87] OIG, *Inspection of the Bureau of Diplomatic Security, Directorate of International Programs* (ISP-I-16-07, February 2016).

[88] OIG, *Compliance — Audit of the Administration and Oversight of Contracts and Grants Within the Bureau of African Affairs* (AUD-CG-14-31, April 26, 2016).

[89] OIG, *Inspection of the Bureau of Information Resource Management, Operations, Vendor Management Office* (ISP-I-16-03, November 2015).

[90] *Ibid.*

FINANCIAL MANAGEMENT

CHALLENGE

The Department continues to make progress resolving financial management concerns, but challenges remain. Persistent lapses in internal controls and vulnerabilities in the purchase card program need to be addressed.

The Department's financial activities occur in approximately 270 locations in 180 countries. Business transactions are conducted in over 135 currencies and even more languages and cultures. Hundreds of financial and management professionals around the globe allocate, disburse, and account for billions of dollars in annual appropriations, revenues, and assets. The Department provides financial management services to 45 U.S. Government agencies, which are located in every corner of the world and which require services 24 hours a day, seven days a week.[91] The Department manages one of the U.S. Government's most complex financial operations and, to its credit, received an unmodified ("clean") audit opinion on its FY 2014 and FY 2015 financial. Accordingly, OIG's efforts with respect to this management challenge focused on helping Department identify remaining vulnerabilities to fraud, waste, and abuse. Although the Department's system is increasingly efficient and streamlined, in FY 2016, OIG found specific lapses related to management controls as well as vulnerabilities in the Department's purchase card program.

Shortcomings in Processes Used to Identify Management Control Deficiencies

Effective management control systems play a key role in ensuring that the Department produces accurate financial statements and is able to achieve its objectives through effective stewardship of public resources. In FY 2016, OIG identified deficiencies in processes used to identify management control deficiencies.

The Department's statement of assurance process, along with information from financial audits and other sources, informs the Secretary of State's opinion about the effectiveness of the management controls and the existence of any material weaknesses or significant deficiencies.[92] During an inspection of the Bureau of International Organizations, OIG found that it had not analyzed management controls related to all of its programs and activities before reporting, through the statement of assurance process, that no material weaknesses or significant deficiencies existed. [93] OIG's review of the statement of assurance process found that guidance sent to bureaus and embassies on the process was insufficient, that coordination between and

[91] Department of State, *Fiscal Year 2014 Department of State Agency Financial Report* (November 2014).

[92] The FMFIA of 1982 and OMB Circular A-123 require that the Secretary annually list the Department's material weaknesses and significant deficiencies and certify that an evaluation of management controls was conducted, that controls comply with standards, and that controls provide reasonable assurance that the Department's programs are effectively carried out in accordance with law.

[93] OIG, *Inspection of the Bureau of International Organizations* (ISP-I-16-02, October 2015).

among bureaus on management control deficiencies was lacking, and that areas of significant risk were not shared with bureaus and missions.[94] Similarly, OIG's review of the Bureau of Consular Affairs' process for identifying control weaknesses at overseas missions found that, although the bureau's data provided a useful snapshot, it was not designed to meet governing management control standards.[95] Data collected was not aggregated or analyzed to help mitigate risk, data was not shared with higher-level management, and data did not allow for continuous monitoring of consular operations.

Lapses in Management Controls

In FY 2016, OIG identified management control issues at various levels of the Department, including financial reporting, line of sight standards, and employee supervision.

The *Independent Auditor's Report on Internal Control Over Financial Reporting* noted the following significant deficiencies: financial reporting, property and equipment, budgetary accounting, validity and accuracy of unliquidated obligations (ULOs) and information technology.[96] These same deficiencies were identified in 2014. The independent auditor's report on the Department's 2015 and 2014 financial statements noted that the Department's internal controls were not effective to ensure that ULOs were consistently and systematically evaluated for validity and deobligation. In addition, funds that could have been used for other purposes may have remained in unneeded obligations.[97]

In addition, although the evaluation of program results is a key internal control that enables decision-makers to make informed budgetary and programmatic decisions, OIG found bureaus do not always conduct such evaluations. During one inspection,[98] OIG found that the efforts of the Bureau of International Organization Affairs to evaluate $340 million in foreign assistance voluntary contributions paid to international organizations were insufficient, hindering the bureau's ability to make budgetary decisions, measure results, and ensure accountability to U.S. taxpayers. This follows an earlier OIG review that determined that 16 of 39 bureaus had not conducted program evaluations as required and that some bureaus did not consistently incorporate evaluation findings into the budget and strategic planning processes.[99]

When conducting reviews of Department operations and compliance with prior OIG recommendations, OIG identified instances of management control lapses related to process and employee supervision. OIG found consular sections that did not comply with the Department's line of sight standards, which were created to ensure adequate supervision of the

[94] OIG, *Review of Statements of Assurance Process* (ISP-I-15-37, September 2015).

[95] OIG, *Review of the Consular Annual Certification of Management Controls Process* (ISP-I-16-01, October 2015).

[96] OIG, *Independent Auditor's Report on Internal Control Over Financial Reporting* (AUD-FM-16-10, November 2015).

[97] OIG, *Independent Auditor's Report on Closing Package Financial Statements* (AUD-FM-16-09, November 2015).

[98] OIG, *Inspection of the Bureau of International Organization Affairs* (ISP-I-16-02, October 2015).

[99] OIG, *Review of Department of State Compliance with Program Evaluation Requirements* (ISP-I-15-36, September 2015).

visa adjudication process and identify any occurrences of theft or malfeasance.[100] In addition, the Department had not yet complied with a 2015 OIG recommendation that the Department revise decision criteria for tenure and promotion in the Foreign Service to ensure that mid- and senior-level Foreign Service Officers address misconduct by their subordinates. Without such criteria and a revision in instructions to employee evaluation reports, managers may not realize the importance of holding supervisors responsible for addressing subordinates' misconduct .[101]

Vulnerabilities in the Purchase Card Program

In an assessment of the Department's purchase card program, OIG concluded that the risk of illegal, improper, or erroneous use in the program is "high" based on a variety of factors, including the large size of the program, the absence of internal controls, a lack of training, results from previous audits, OIG's Office of Investigations observations, and violation reports.[102]

OIG's management assistance report on the Department's annual purchase card program reviews found that 53 percent of overseas purchase card coordinators in FY 2014 either failed to perform mandatory annual reviews of their purchase card programs or did not respond to a request for that information.[103] The monetary value of goods and services obtained using purchase cards at those non-compliant and non-responsive posts totaled almost $34 million. FY 2016 OIG inspections also identified numerous deficiencies related to bureau and post purchase card programs. Inspectors found a lack of enforcement in advance-approval of purchase card actions[104] and an absence of annual purchase card reviews and card holder training.[105] The Department's Bureau of Administration does not monitor bureau and post compliance with the annual purchase card review requirement but should do so consistent with its own internal policies[106] to identify fraud, areas of risk, and other trends.

Recent Department Actions to Address Deficiencies Related to Financial Management and the Annual Statement of Assurance

Management Controls and Oversight

- The Department issued guidance defining the procedures for reporting deficiencies between posts and regional bureaus and requiring the chief of mission to designate a management control coordinator at the beginning of each fiscal year.[107]

---

[100] OIG, *Inspection of Embassy Tashkent* (ISP-I-16-12A, March 2016); OIG, *Inspection of Embassy Ashgabat* (ISP-I-16-13A, March 2016).

[101] OIG, *Compliance Follow-up Review of the Review of the Department of State Disciplinary Process* (ISP-C-16-16, April 2016).

[102] OIG, *Information Report: Department of State 2015 Purchase Card Risk Assessment* (AUD-FM-16-23, December 2015).

[103] OIG, *Management Assistance Report: Annual Purchase Card Program Reviews* (ISP-I-16-04, January 2016).

[104] OIG, *Inspection of the Bureau of International Organizations* (ISP-I-16-02, October 2015).

[105] OIG, *Inspection of Embassy Cairo* (ISP-I-16-15A, April 2016).

[106] 1 FAM 212.2.

[107] OIG, *Review of the Statement of Assurance Process* (ISP-I-15-37, September 2015).

- The Department revised the FY 2016 annual consular management control survey questionnaire to improve the accuracy of individual post reporting and is in the process of deploying a commercial, off-the-shelf toolkit that will automate the worldwide monitoring of individual post performance of consular management control oversight.
- In recognition of the need to incorporate program evaluation findings into the budget and strategic planning processes, the Department revised the Bureau Resource Request guidance for FY 2018 to include sections to discuss bureau accomplishments. The data used to assess performance for diplomatic engagement funding requests will be aligned with each bureau's Functional Bureau Strategy and Joint Regional Strategy goals and objectives.[108]

Vulnerabilities in the Purchase Card Program

- The Department's Worldwide Purchase Card Program Manual mandates annual purchase card program reviews. After fraud was discovered at Embassy Kinshasa, the embassy resumed use of the recommended purchase card reconciliation procedures and added an additional control (a monthly peer review of credit card invoices).[109]
- The Department designated the Bureau of Administrations' Office of Acquisitions Management as the single office with responsibility for oversight of the Worldwide Purchase Card Program.[110]

[108] OIG, *Review of the Department of State Compliance with Program Evaluation Requirements* (ISP-I-15-36, September 2015).

[109] OIG, *Inspection of Embassy Kinshasa* (ISP-I-16-19A, June 2016).

[110] OIG, *Management Assistance Report: Annual Purchase Card Program Reviews* (ISP-I-16-04, January 2016).