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

"STATE DEPARTMENT AND USAID MANAGEMENT CHALLENGES AND OPPORTUNITIES FOR THE NEXT ADMINISTRATION"

STATEMENT BY
STEVE A. LINICK

INSPECTOR GENERAL FOR THE U.S. DEPARTMENT OF STATE
AND THE BROADCASTING BOARD OF GOVERNORS

BEFORE THE COMMITTEE ON FOREIGN RELATIONS,
SUBCOMMITTEE ON STATE DEPARTMENT AND
USAID MANAGEMENT, INTERNATIONAL OPERATIONS,
AND BILATERAL INTERNATIONAL DEVELOPMENT

UNITED STATES SENATE
DECEMBER 8, 2016

Chairman Perdue, Ranking Member Kaine, and Members of the Subcommittee, thank you for inviting me to testify today regarding the work of the Office of Inspector General (OIG) for the Department of State (Department) and the Broadcasting Board of Governors (BBG). I will highlight some of our recent oversight work, our continuing initiatives, and the challenges we face in performing efficient and effective oversight. I will also address the results and impact of our work. At the outset, I would also like to thank this Subcommittee for its interest in and support of OIG's work. In particular, I would like to take this opportunity to thank Members of this Subcommittee for sponsoring legislation intended to expand our hiring authority and our ability to obtain information regarding misconduct by senior Department personnel. This legislation is critical to our operation.

I. STATE OIG'S MISSION AND OVERSIGHT EFFORTS

It is my honor to have led the State OIG for the last three years, and I am pleased to have this chance to update you on the work we have performed since I last testified before this Subcommittee in April 2015.

As I explained at that time, OIG's mandate is extensive and requires us to oversee both Department and BBG programs and operations, which include more than 70,000 employees and over 270 overseas missions and domestic entities. These agencies are funded through combined annual appropriations, fees, and other income of approximately $43 billion. Moreover, one important difference between State OIG and most other OIGs is that we are statutorily required to periodically inspect and audit every domestic and overseas operating unit around the world.

In recent reports, we have identified some of the top challenges that the Department faces. Today, I will focus particularly on the protection of people and facilities, the security of sensitive information around the world, and the management of contracts and grants. These three issues represent a significant part of the work that we have done over the past eighteen months.

Protecting People and Facilities

As testified previously, one of OIG's top priorities is protecting those who work for the Department around the world. OIG has always inspected physical security at overseas posts, but, since the September 2012 attacks on U.S. diplomatic facilities and personnel in Benghazi, Libya, we are now expending additional resources on this critical issue. In 2015 alone, personnel and property experienced attacks in Bangladesh, Burundi, Canada, Central African Republic, Iraq, Mali, the Philippines, South Korea, Timor-Leste, Turkey, and Yemen.[1] These 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.

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

Although the Department has continued to make improvements in overseas safety and security over the past 18 months, challenges remain. Through our inspection and audit work, OIG continues to find deficiencies that put our people at risk. Given the sensitive nature of OIG's work in this area, many of the reports related to safety and security are classified, and my testimony today will be based solely on information that is publicly available.

Health and safety concerns were a recurring theme in OIG's FY 2016 reports. Our work in these areas covered a wide range of risks. For example, OIG found deficiencies in seismic risk mitigation in embassy residences[2] and a lack of occupational safety and health approvals to ensure that hazards are addressed before overseas housing is occupied.[3] OIG also identified life, health, and safety risks to building occupants due to hazardous spikes in electrical current in both the office and apartment complexes at Embassy Kabul.[4] In another report, OIG 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.[5] The Bureau of Overseas Buildings Operations (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. Although the Department has acknowledged that driver behavior contributes to vehicle fatalities and that solutions must center on training, OIG recommended that the Department take additional action to address the issue by establishing a mandatory training requirement on armored vehicle safe-driving techniques for all overseas professional chauffeurs and incidental drivers who operate such vehicles.[6]

Another area of focus has been emergency action plans. These plans and associated processes are important because planning and preparation can make the difference between life and death in a crisis situation. 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.[7] Without this information, embassies and consulates cannot properly plan for emergencies and may be hindered in their responses to actual crises. OIG also 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.[8] 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.[9] Without adequate staff training and a properly documented

---

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

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

[4] 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).

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

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

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

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

[9] 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).

and tested emergency action plan, embassies and consulates cannot effectively mitigate the risks that a disaster or unforeseen incident poses to its operations.

Finally, maintaining sufficient physical security at overseas facilities is an important aspect 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.[10] In recent years, the Department has developed new tools to identify and track physical security deficiencies overseas; however, the Department needs to take additional action. 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.[11]

Conducting oversight to protect people and facilities is one of our most important functions. Consequently, we will continue to coordinate with the Department to bring security deficiencies and areas for improvement to its attention and offer recommendations to address these critical vulnerabilities. By conducting both our statutorily mandated inspections and targeted audits and evaluations, OIG helps safeguard the lives of people who work in or visit our posts abroad.

Information Security and Management

The Department depends on information systems and electronic data to carry out essential functions that are critical to its mission. The Department is entrusted with sensitive information, both classified and unclassified. The security of these systems is vital to protecting national and economic security, public safety, and the flow of commerce.[12] According to the Office of Management and Budget, the Department has spent several billion dollars in the past 5 years on software tools, IT equipment, and professional expertise. However, given the complexity and sensitivity of the Department's IT apparatus and the security breaches it has experienced, IT security and management continues to be a significant management challenge.

In FY 2016, OIG reported significant weaknesses in the Department's cybersecurity incident response and reporting program.[13] 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.

---

[10] 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).
[11] *Ibid.*
[12] OIG, *Audit of the Department of State Information Security Program* (AUD-IT-16-16, November 2015).
[13] OIG, *Management Assistance Report: Department of State Incident Response and Reporting Program* (AUD-IT-16-26, February 2016).

OIG also 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.[14] This is a critical issue because, if an unneeded account remains active, an intruder could gain access to sensitive information that could compromise the integrity of the Department's network and cause widespread damage across its IT infrastructure. This problem exists, in part, because the Department does not have a centralized process for AD account management. This issue is exacerbated by the fact that, as we also reported, the Department's Chief Information Officer, the head of the Bureau of Information Resource Management (IRM), is not properly positioned within the organization to ensure that the Department's information security program is effective.

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.[15] OIG has reported that the Department lacks effective risk management for all phases of the system development lifecycle.[16] These problems persist. For example, in the October 2015 inspection of IRM's Vendor Management Office (VMO), OIG found that VMO did not consistently implement the system that provides the framework for integrating IT project schedules. This inconsistency led to inadequate bureau coordination, incomplete project data, and limited visibility on projects, activities, and risk.

Finally, on a related point, the last time I testified before this Subcommittee, I described OIG's vulnerable IT network as a major challenge. Vulnerabilities in the Department's unclassified network directly affected OIG's IT infrastructure, which was part of the same network. I testified that the fact that the contents of our unclassified network could be easily accessed and potentially compromised placed our independence at unnecessary risk and did not reflect best practices within the IG community. I am pleased to report that OIG recently established its own independent IT network to mitigate these risks.

[14] OIG, *Management Assistance Report: Inactive Accounts within the Department of State's Active Directory* (AUD-IT-16-37, June 2016).
[15] OIG, *Audit of the Department of State Information Security Program* (AUD-IT-16-16, November 2015).
[16] OIG, *Inspection of the Bureau of Information Resource Management, Operations, Vendor Management Office* (ISP-I-16-03, October 2015).

Oversight of Contracts and Grants

OIG has focused on oversight of contracts and grants, an area where the Department spends substantial resources. The Department's obligations in FY 2016 included approximately $15.4 billion for contracted services and $18.4 billion in grants and fixed charges.[17] As it did the last time I testified, the Department faces continuing challenges managing its contracts, grants, and cooperative agreements, particularly as these vehicles become increasingly complex. The Department needs to ensure that contractors and grantees are properly selected, work is properly conducted and monitored, objectives of the grant or contract are achieved, and costs are effectively contained. As with ensuring the safety of its personnel, management of grants and contracts is especially challenging in conflict areas, which present unique obstacles to effective oversight.

Although the Department has addressed some problems, weaknesses continue to occur in other areas. In FY 2016, OIG issued several management assistance reports addressing the Department's oversight of contracts and grants, and OIG's Office of Investigations opened more than 30 cases related to contract and procurement fraud.

During FY 2016, OIG identified 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, failed to comply with Department guidance and Federal regulations.

Audits of contracts in Iraq revealed millions of dollars in questioned and unsupported costs and unallowable fees. For example, 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 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.[18]

With regard to grants, OIG audits and inspections identified the need for improved management and monitoring of grantees. For example, in an audit of the Bureau of Political-Military Affairs' (PM) grantees,[19] OIG reported that $2.8 million of $15.8 million in grant expenditures were unsupported or unallowable, as defined by Federal policies. OIG reported that these questioned costs occurred, in part, because PM's grant monitoring process was not

[17] USASpending, <www.usaspending.gov>, accessed on November 21, 2016.
[18] OIG, *Audit of Task Orders for the Union III Compound Awarded Under the Operations and Maintenance Support Services* (AUD-MERO-16-41, July 2016).
[19] OIG, *Audit of the Bureau of Political-Military Affairs Federal Assistance Awards* (AUD-SI-16-49, September 2016).

designed to prevent or detect unallowable and unsupported costs. In particular, PM did not independently verify that all award recipients had sufficient financial management controls in place to prevent unsupported and unallowable costs.

Finally, OIG's inspection of the Bureau of Democracy, Human Rights, and Labor (DRL) programs in Iraq noted the challenges the Department faces in managing grants in conflict areas. 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.[20] 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.

II. CONTINUING INITIATIVES

Nineteen months ago, I described several new initiatives. These initiatives are no longer "new"; rather, they are an integral part of our day-to-day work processes.

First, I earlier testified that OIG had begun making use of management assistance reports and management alerts to bring specific issues to the attention of Department and BBG management quickly and without waiting for the conclusion of longer-term audits or inspections. Since I last spoke with you, OIG has issued four management alerts,[21] which I personally sign, and twenty-five management assistance reports.[22] These reports are an important part of our oversight efforts.

Next, in April 2015, I discussed the role of the Office of Evaluations and Special Projects (ESP), which was established in 2014. I am pleased to report that ESP has issued nine reports and two management alerts and continues to focus on systemic issues. In addition, this office has continued to expand our efforts to meet the requirements of the Whistleblower Protection Enhancement Act of 2012 and related statutes. In particular, the office's whistleblower ombudsman has expanded our outreach and provided extensive information to Department and BBG employees, grantees, and contractors. ESP also is responsible for conducting investigations of allegations of administrative misconduct, as well as retaliation, under the pilot program for

---

[20] 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).

[21] 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); OIG, *Management Alert: Evacuation of Embassy Tripoli* (MA-15-02, July 2015); OIG, *Management Alert: Broadcasting Board of Governors Significant Management Weaknesses* (MA-15-01, May 2015); OIG, *Management Alert: Information Security in the Worldwide Refugee Admissions Processing System* (MA-17-03, December 2016).

[22] *See, e.g.*, OIG, *Management Assistance Report: Mandatory Disclosure Language in Department of State Grants and Assistance Agreements* (INV-15-02, December 2015); OIG, *Management Assistance Report: Contract Management – Lessons Learned From Embassy Kabul, Afghanistan, Operations and Maintenance Contract* (AUD-MERO-17-04, October 2016).

contractor and grantee employee whistleblowers and has issued eight reports under this program.

Finally, our work in connection with overseas contingency operations is now an established, well-integrated part of OIG's overall work. I am the Associate Inspector General for the overseas contingency operations in Afghanistan (Operation Freedom Sentinel) and Iraq (Operation Inherent Resolve), and our staff is working closely with the Department of Defense and USAID OIGs to oversee those operations. Since I last spoke before this Subcommittee, I have appointed an assistant inspector general who is responsible for overseeing the work of our OCO staff. Besides working with the other agencies with oversight responsibility, this staff coordinates closely with OIG's offices of audit and inspections to make the most effective and efficient use of resources. To date, our major oversight efforts have focused on auditing and evaluating bureaus and embassies that engage or support counter-ISIL activities. We have also emphasized contract and grant monitoring in contingency and high-threat environments. In addition, we issued a "Lessons Learned" guide for program managers at the Department of State operating in critical and high-threat environments. During FY 2016, OIG issued 31 oversight products related to OCOs, and we currently have more than 30 ongoing projects.

III. CHALLENGES

Unlike other OIGs, my office is not always afforded the opportunity to investigate allegations of criminal or serious administrative misconduct by Department employees. Department components, including the Bureau of Diplomatic Security (DS), are not required to notify OIG of such allegations that come to their attention. For example, current Department rules provide that certain allegations against chiefs of mission shall be referred for investigation to OIG *or* DS. That guidance further states that "[in] exceptional circumstances, the Under Secretary for Management may designate an individual or individuals to conduct the investigation."[23] Thus, DS or the Under Secretary may initiate an investigation without notifying us or providing us with the opportunity to evaluate the matter independently and become involved, if appropriate. Accordingly, OIG cannot undertake effective, independent assessments and investigations of these matters as envisioned by the IG Act.

We have been negotiating with the Department for at least two years to address these limitations on our ability to conduct oversight, but the problem persists. Although the Department has begun providing OIG with some information, the process for doing so has not been formalized, and the information is provided to us selectively. That being said, I want to acknowledge and thank both Chairman Perdue and Ranking Member Kaine for sponsoring legislation that would address this limitation.[24] Unfortunately, the need for a legislative fix remains. I welcome your continued support as this Congress ends and the new Congress begins next year.

[23] 3 Foreign Affairs Manual 4322.2.

[24] Improving Department of State Oversight Act of 2015, S.1527, 114th Congress (2015).

IV. IMPACT

OIG embraces our mission to protect people and information, although these efforts rarely result in a monetary return on investment. At the same time, through our audits, evaluations, inspections, and investigations, OIG returns real value to U.S. taxpayers. Since my arrival three years ago, we have issued 317 reports, which included audits of annual financial statements, procurement activities, and funds management. During this same period, we identified more than $300 million in taxpayer funds that could be put to better use and questioned costs. Additionally, our criminal, civil, and administrative investigations resulted in the imposition or identification of more than $82 million in fines, restitution, recoveries, and other monetary results.

OIG also provides important non-financial benefits. By helping the Department improve its security, OIG's work helps safeguard the lives of people who work in or visit our posts abroad. Success in this area is not reflected in our financial statistics, but our security work is a source of immense pride because its employees are, of course, the Department's most valuable assets. Our oversight provides other non-monetary benefits as well. These include our health and safety work, our investigations that help ensure that Department employees conduct themselves appropriately, and our work to strengthen the integrity of the programs, operations, and resources that are at the foundation of the Department's ability to help preserve our national security. Indeed, the work of our talented staff in reviewing security and leadership at our overseas and domestic posts has significant and positive effects on the lives and well-being of employees throughout the Department. That is what motivates our employees, many of whom are on the road or serve overseas for extended periods, sometimes at high-threat posts.

In conclusion, I want to thank Chairman Perdue, Ranking Member Kaine, and the other Members of the Subcommittee here today for the opportunity to testify. I also want to emphasize that OIG's accomplishments are a credit to the talented and committed staff that I have had the privilege to lead, and I also want to take this moment to thank them for their hard work. I take my statutory requirement to keep the Congress fully and currently informed seriously, and I appreciate your interest in our work and for providing me the opportunity to articulate the challenges faced by my office. I look forward to your questions.