OIG Office of Inspector General

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

STATEMENT BY

STEVE A. LINICK

INSPECTOR GENERAL FOR THE U.S. DEPARTMENT OF STATE

AND THE BROADCASTING BOARD OF GOVERNORS

BEFORE THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

U.S. SENATE

FIRST SESSION, 114TH CONGRESS

IMPROVING THE EFFICIENCY, EFFECTIVENESS, AND INDEPENDENCE OF INSPECTORS GENERAL

FEBRUARY 24, 2015

Chairman Johnson, Ranking Member Carper, and Members of the Committee, 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). In my testimony, I will highlight some of our recent oversight work, our new initiatives, and the challenges we face in performing our oversight. I will also address the overall positive results and impact of OIG work.

I. STATE OIG'S MISSION AND OVERSIGHT EFFORTS

It is my honor to have led the State OIG for the past 17 months—since the end of September 2013. OIG's mandate is broad and comprehensive, involving oversight of the full scope of the Department and BBG programs and operations, including more than 72,000 employees and 280 overseas missions and domestic entities, as well as the U.S. Section of the International Boundary and Water Commission. These agencies are funded through combined annual appropriations of approximately $15 billion and nearly $7 billion in consular fees and other earned income. OIG also is responsible for full or partial oversight of an additional $17 billion in Department-managed foreign assistance.

State OIG differs from most OIGs in that it has a mandated inspection function. We are statutorily required to periodically audit and inspect every domestic and overseas operating unit around the world. Since the beginning of my tenure, we have redoubled our efforts to address some of the top challenges of the Department, including the protection of people and facilities, the management of contracts and grants, and the security of sensitive information around the world. I will elaborate on each of these:

Improving Security

Protecting the people who work for the Department is a top priority for the Department and for OIG. OIG has inspected physical security at overseas posts for years; however, since the September 2012 attacks on U.S. diplomatic facilities and personnel in Benghazi, Libya, OIG has significantly stepped up its oversight efforts related to security, including targeted audits and evaluations. We help safeguard the lives of people who work in or visit our posts abroad by performing independent oversight to help the Department improve its security posture. Unlike many of our other oversight activities, as well as more traditional Government-wide work conducted by the Inspector General (IG) community, we cannot attach a dollar-value metric to our efforts related to physical security. Achievement in this area is not reflected in our "return on investment" statistics. However, our oversight successes are a source of great satisfaction, and to the degree that unreasonable risk persists, OIG will vigorously continue to highlight any deficiencies to the Department and to Congress.

Although the Department has made improvements on overseas security, challenges remain. Through our inspection and audit work, OIG continues to find security deficiencies that put our people at risk. Those deficiencies include failing to observe set-back and perimeter requirements

and to identify and neutralize weapons of opportunity. Our teams also uncover posts that use warehouse space and other sub-standard facilities for offices, another security deficiency.[1] Under the Department's security rules, office space must meet more stringent physical security standards than warehouse space. Our audit[2] of the Local Guard Program found that firms providing security services for embassy compounds were not fully vetting local guards they hired abroad, placing at risk our posts and their personnel. In other audits, we found that the Bureau of Diplomatic Security (responsible for setting standards) and the Bureau of Overseas Buildings Operations (responsible for constructing facilities to meet those standards) often do not coordinate adequately to timely address important security needs.[3] Those bureaus have taken steps to improve their communication and coordination. OIG will closely monitor whether these steps actually sustain improved joint performance to mitigate security vulnerabilities.

OIG has also examined the Department's handling of significant security breaches that resulted in the deaths of U.S. Government personnel. For example, in September 2013, OIG published a report[4] on its Special Review of the Accountability Review Board (ARB). As you know, the Secretary of State convenes an ARB when serious injury, loss of life, or significant destruction of property at or related to a U.S. Government mission abroad has occurred. The most recent ARB was convened following the 2012 attacks and tragic events in Benghazi. OIG's Special Review examined the process by which the Department's ARBs are established, staffed, supported, and conducted as well as the manner in which the Department tracks the implementation of ARB recommendations. We found that follow-through on long-term security program improvements involving physical security, training, and intelligence-sharing lacked sustained oversight by Department principals. Over time, the implementation of recommended improvements slows. The lack of follow-through explains, in part, why a number of Benghazi ARB recommendations mirror previous ARB recommendations. This underscores the need for a sustained commitment by Department principals to ensure that ARB recommendations are timely and effectively carried out.

OIG also continues to increase its focus on security issues. OIG currently is following up on the Department's compliance with OIG recommendations in the ARB Special Review. OIG will also review the Department's reported compliance with the 29 recommendations in the Benghazi ARB report. In addition, planned FY 2015 security audits include an audit of the approval and certification process used to determine employment suitability for locally employed staff and contracted employees, an audit of emergency action plans for U.S. Missions in the Sahel region of Africa, and an audit of the Vital Presence Validation Process (VP2) implementation. VP2 is the Department's formal process for assessing the costs and benefits of maintaining its presence in

[1] *Review of Overseas Security Policy Board Exceptions and Secure Embassy Construction and Counterterrorism Act of 1999 Waivers* (ISP-I-13-06, January 2013).
[2] *Audit of Contractor Compliance With and Department of State Oversight of the Process Required for Vetting Local Guards* (AUD-HCI-14-24, June 2014).
[3] *Inspection of the Bureau of Diplomatic Security, High Threat Programs Directorate* (ISP-I-14-23, September 2014); *Compliance Follow-up Review of the Bureau of Overseas Buildings Operations* (ISP-C-11-26, May 2011); *Audit of the Process to Request and Prioritize Physical Security-Related Activities at Overseas Posts* (AUD-FM-14-17, Mar. 2014).
[4] *Special Review of the Accountability Review Board Process* (ISP-I-13-44A, September 2013).

dangerous locations around the world. Finally, we will continue to emphasize security concerns as we inspect the International Programs Directorate of the Bureau of Diplomatic Security.

Improving Oversight of Contracts and Grants

Contracts and grants are critical to the Department's mission. The Department's obligations in FY 2014 equaled approximately $9 billion in contractual services and $1.5 billion in grants, totaling approximately $10.5 billion.[5] However, the Department faces challenges managing its contracts, grants, and cooperative agreements. These challenges have come to light repeatedly in OIG audits, inspections, and investigations over the years. They were highlighted in two recent OIG Management Alerts that I provided to senior Department officials.

In FY 2014, more than 50 percent of post or bureau inspections contained formal recommendations to strengthen controls and improve administration of grants. In our March 2014 Management Alert[6] focusing on contract management deficiencies, we reported that over the past 6 years, files relating to Department contracts with a total value of more than $6 billion were either incomplete or could not be located at all. In a September 2014 Management Alert[7] on grant management deficiencies, we highlighted weaknesses in oversight, insufficient training of grant officials, and inadequate documentation and closeout of grant activities. In FY 2012 alone, the Department obligated more than $1.6 billion for approximately 14,000 grants and cooperative agreements worldwide.[8] This is a significant outlay of taxpayer funds, which makes oversight and accountability even more critical. Grants present special oversight challenges because, unlike contracts, they do not generally require the recipient to deliver specific goods or services that can be measured.

The Department has agreed to adopt most of OIG's recommendations in these Management Alerts. OIG will continue to monitor the Department's efforts and seek additional improvements in this important area.

In FY 2015, OIG plans on issuing, among others, audits involving non-lethal aid and humanitarian assistance in response to the Syrian crisis, the Iraq Medical Services Contract, and the Bureau of International Narcotics and Law Enforcement's Embassy Air Wing Contract in Iraq.

Enhancing Information Security

Another top management challenge concerns information security. The Department is entrusted to safeguard sensitive information, which is often targeted by multiple sources, including terrorist and criminal organizations. The Department is responsible for preserving and protecting classified and other sensitive information vital to the preservation of national security in high-risk environments across the globe. OIG's assessments of the Department's cybersecurity

[5] USASpending, <www.usaspending.gov>, accessed on February 19, 2015.
[6] *Management Alert: Contract File Management Deficiencies* (MA-A-0002, March 20, 2014).
[7] *Management Alert: Grants Management Deficiencies* (MA-14-03, September 26, 2014).
[8] U.S. Government Accountability Office, *Implementation of Grants Policies Needs Better Oversight* (GAO-14-635, July 2014).

programs have found recurring weaknesses and noncompliance with the Federal Information Security Management Act (FISMA) with respect to its unclassified systems. In a November 2013 Management Alert,[9] we raised concerns and found inadequate access controls, ineffective security scanning, and weaknesses in cybersecurity management (including absence of a strategic plan).

Our work in the information security area is ongoing. Since my arrival, OIG has arranged for penetration testing of the Department's unclassified networks in order to better assess their vulnerability to attack.

II. NEW OIG INITIATIVES

Since joining OIG, I have implemented a number of new initiatives to enhance the effectiveness and efficiency of OIG's independent oversight of the Department's programs and operations:

Management Alerts and Management Assistance Reports

Soon after my arrival, we began to issue Management Alerts[10] and Management Assistance Reports.[11] They are intended to alert Department leadership to significant issues that require immediate corrective action. For example, we issued two Management Assistance Reports recommending that the Department take immediate action (for example, termination) against certain grantees for misuse of grant funds. In addition, and as mentioned above, we issued Management Alerts[12] relating to serious problems in the areas of grant and contract management and information security. The response from the Department to these products has been favorable as they have concurred with most of our recommendations.

Moreover, Congress has also recognized their value. The explanatory statement to the FY 2015 Omnibus Appropriations bill included language directing the Secretary of State to submit to Congress a report detailing the status of each of the recommendations included in OIG's FY 2014 Management Alerts.

---

[9] *Management Alert: OIG Findings of Significant, Recurring Weaknesses in Department of State Information System Security Program* (MA-A-0001, November 12, 2013).

[10] *Management Alert: OIG Findings of Significant, Recurring Weaknesses in Department of State Information System Security Program*, (MA-A-0001, January 2014); *Management Alert: Contract File Management Deficiencies* (MA-A-0002, March 2014); *Management Alert: Grants Management Deficiencies* (MA-14-03, September 2014).

[11] *Management Assistance Report: Concerns with the Oversight of Medical Support Service Iraq Contract No. SAQMMA11D0073* (AUD-MERO-15-20, December 23, 2014); *Management Assistance Report: Grant Improprieties by Nour International Relief Aid* (AUD-CG-15-19, January 15, 2015); *Management Assistance Report: Termination of Construction Grants to Omran Holding Group* (AUD-CG-14-37, September 18, 2014).

[12] *Management Alert: Contract File Management Deficiencies* (MA-A-0002, March 20, 2014); *Management Alert: Grants Management Deficiencies* (MA-14-03, September 26, 2014); *Management Alert: OIG Findings of Significant and Recurring Weaknesses in the Department of State Information System Security Program* (MA-A-0001, November 12, 2013).

Office of Evaluations and Special Projects

The Office of Evaluations and Special Projects (ESP) was established in 2014 to enhance OIG's oversight of the Department and BBG. In particular, ESP undertakes special evaluations and projects and complements the work of OIG's other offices by further developing the capacity to focus on broader, systemic issues. For example, in October 2013, ESP published a Review of Selected Internal Investigations by DS,[13] which addressed allegations of undue influence by Department management. Currently, ESP is conducting a joint review with the Department of Justice's OIG of the handling of the use of lethal force during a counternarcotics operation in Honduras in 2012.

Increased Emphasis on Whistleblower Protections

OIG is also using ESP to improve OIG's capabilities to meet statutory requirements of the Whistleblower Protection Enhancement Act of 2012 and other whistleblower initiatives. Department employees, employees of contractors and grantees, and others have been encouraged to report fraud, waste, abuse, and misconduct. Such reporting must take place without fear of retaliation. We have designated an ombudsman (a senior ESP attorney) for these purposes. We also produced an educational video and published a guide regarding whistleblower protections on our website.[14]

Oversight of Overseas Contingency Operations

The IG community was recently tasked, through an amendment to the Inspector General Act of 1978 (IG Act), with additional responsibility for overseeing current and future overseas contingency operations. Approximately 8 weeks ago, Jon T. Rymer, the Inspector General for the Department of Defense (DoD), was appointed Lead Inspector General for Operation Inherent Resolve (OIR)—the U.S.-led overseas contingency operation directed against the Islamic State of Iraq and the Levant (ISIL). Mr. Rymer subsequently appointed me as Associate Inspector General in charge of oversight. Three OIGs (State, DoD, and USAID) have dedicated staff to this important project. We are working jointly on: (1) strategic planning, to provide comprehensive oversight of all programs and operations in support of the OIR; (2) program management, to track, monitor, and update information provided by our agencies in support of the OIR; and (3) communications, to collect information and prepare periodic reports for Congress on projects related to the OIR. Relatedly, we are in the process of establishing a hotline dedicated to the contingency operation and developing joint investigative capabilities for OIR oversight.[15]

---

[13] *Review of Selected Internal Investigations Conducted by the Bureau of Diplomatic Security* (October 2014, ESP-15-01).

[14] OIG, Whistleblower Protection, <http://oig.state.gov/hotline/whistleblower>.

[15] OIG did not receive additional funding for ISIL oversight in 2015. In 2016, OIG received a total budget increase of $9 million, which the OMB passback stated is intended "to address any expanded oversight requirements resulting from the FY 2015 counter-ISIL OCO budget amendment and the Counterterrorism Partnership Fund (CTPF), if enacted." Until the scope of the ISIL response is fully developed, OIG cannot predict the resources needed for effective oversight.

Data and Technology

OIG is developing an automated evidence tracking system to enhance evidence processing accuracy and efficiency, and employee computer forensic and data processing procedures in order to significantly reduce agents' time and investigative hours. Further, we are building the capacity of our new data analytics group and developing a fusion cell consisting of special agents, forensic auditors, criminal analysts, and computer specialists. This group of specialists will enable all of our divisions to proactively analyze financial data to identify potential vulnerabilities in Department programs and processes and perform fraud risk assessments.

Suspension and Debarment

We have enhanced our efforts to identify and refer appropriate cases to the Department for suspension and debarment. Our Offices of Investigations and Audits prepare detailed suspension and debarment recommendation packages, in consultation with our Office of General Counsel, including referral memoranda summarizing all relevant facts and setting forth the specific grounds for suspension or debarment and submit their packages to the Department's Suspension and Debarment Officials (SDOs) for action. Between 2011 and 2014, OIG referred 128 cases to the Department for action.

New Locations

For reasons of oversight efficiency and to have "boots on the ground" at key financial locations, OIG intends in the near term to locate staff in Charleston, South Carolina, where one of the Department's Global Financial Services Center resides, and in Frankfurt, Germany, the site of one of the Department's Regional Procurement Support Office. Both locations are responsible for billions of taxpayer dollars. These moves will allow OIG to more efficiently and more economically access pertinent information and pursue targeted reviews.

Prosecution of Cases

OIG has initiated a program to place one or more Special Assistant U.S. Attorneys (SAUSAs) in appropriate positions in the Department of Justice in order to prosecute more quickly and effectively cases involving fraud against the Department of State. For example, an OIG attorney-investigator now works as a full-time SAUSA in the U.S. Attorney Office for the Eastern District of Virginia.

III. CHALLENGES IN PERFORMING OVERSIGHT

Finally, I want to address challenges that OIG faces in performing oversight:

Access

In August 2014, I joined 46 of my colleagues from the IG community to write the Chairman and Ranking Members of this Committee as well as your House counterparts to express our support

for the Inspectors General of the Department of Justice, the Peace Corps, and the Environmental Protection Agency with respect to their concerns about access and independence. The principle that oversight necessarily requires complete, timely, and unfiltered access to agency information—and the fact that the IG Act entitles IGs to that information—needs to be upheld whenever challenged. Unfettered and complete access to information is the linchpin that ensures independence and objectivity for the entire OIG community.

At State OIG, we too are committed to ensuring that our work is independent and free from interference. We also recognize the importance of forging productive relationships with Department leadership and decision-makers. At the beginning of my tenure, Secretary Kerry, at my request, issued a Department notice to all employees outlining OIG authorities and obligations under the IG Act and advising staff of our need for prompt access to all records and employees.

Generally, most of our work is conducted with the Department's full cooperation and with timely production of material. However, there have been occasions when the Department has imposed burdensome administrative conditions on our ability to access documents and employees. At other times, Department officials have initially denied access on the mistaken assumption that OIG was not entitled to confidential agency documents. In these instances, OIG ultimately was able to secure compliance but only after delays and sometimes with appeals to senior leadership. These impediments have at times adversely affected the timeliness of our oversight work, resulting in increased costs for taxpayers.

Delays in responding to document requests also occur because the requested information has not been maintained at all or in a manner to allow timely retrieval. Such disorganization of information may negatively impact not only OIG audits, inspections, evaluations, and investigations but also the integrity of Department programs and operations. For example, an OIG Management Alert identified missing or incomplete files for contracts and grants with a combined value of $6 billion.

OIG Network Vulnerabilities

Vulnerabilities in the Department's unclassified network also affect OIG's IT infrastructure, which is part of the same network. We noted in our November 2013 information security Management Alert that there are literally thousands of administrators who have access to Department databases. That access runs freely to OIG's IT infrastructure and creates risk to OIG operations. Indeed, a large number of Department administrators have the ability to read, modify, or delete any information on OIG's network including sensitive investigative information and email traffic, without OIG's knowledge. OIG has no evidence that administrators have actually compromised OIG's network. However, the fact that the contents of our unclassified network may easily be accessed and potentially compromised unnecessarily places our independence at risk. We have begun assessing the best course of action to address these vulnerabilities.

Testimonial Subpoenas and Other Tools

I agree with Department of Justice Inspector General Michael Horowitz and others who support the need for IGs to be able to compel witness testimony. As a former prosecutor, I believe that adding this tool, subject to appropriate oversight and coordination, is essential. I also support other tools to enhance OIG oversight efforts, including exemptions from the Computer Matching and Privacy Protection Act and the Paperwork Reduction Act.

IV. IMPACT OF OIG WORK

Through our audits, evaluations, inspections, and investigations, OIG returns significant value to the taxpayers. In FY 2014, we issued 77 reports, which included audits of annual financial statements, procurement activities, and fund management. During this period, we identified $43.3 million in taxpayer funds that could be put to better use by the Department. Additionally, our criminal, civil, and administrative investigations resulted in the imposition or identification of $75 million in fines, restitution, recoveries, and other monetary results last fiscal year. This was in addition to the $1 billion in financial results[16] from audit- or inspection-related findings and more than $40 million in investigative-related financial results that OIG identified in the previous five fiscal years.

However, these financial statistics do not adequately take into account many of our most significant impacts—the physical safety of people and facilities, the conduct of Department employees, and other fundamental issues involving national security. Indeed, the work of our talented staff in reviewing security and leadership at our overseas and domestic posts has meaningful 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 for long periods of time or who serve for extended periods at high-threat posts.

In conclusion, Chairman Johnson, Ranking Member Carper, and Members of the Committee, thank you again for the opportunity to testify before you today. I take seriously my statutory requirement to keep the Congress fully and currently informed, and I appreciate your interest in our work. I look forward to your questions.

###

[16] Financial results include the value of investigative fines/recoveries and management decisions made on questioned costs and funds put to better use from OIG recommendations.