

# Inspector General's Assessment of Management and Performance Challenges

The *Reports Consolidation Act of 2000*<sup>1</sup> requires that the Department's Performance and Accountability Report include a statement by the Inspector General that summarizes the most serious management and performance challenges facing the Department and briefly assesses the progress in addressing them. The Office of Inspector General (OIG) considers the most serious management and performance challenges for the Department to be in the following areas:



Inspector General,  
Steve A. Linick

1. Protection of People and Facilities
2. Managing Posts and Programs in Conflict Areas
3. Management of Contracts and Grants
4. Information Security and Management
5. Financial Management

## 1 PROTECTION OF PEOPLE AND FACILITIES

Protecting overseas personnel and facilities continues to be a major management challenge for the Department. In 2014, there were 20 attacks on embassy facilities or personnel, including assaults on U.S. employees, small arms and rocket-propelled grenade attacks, and a suicide bombing at the Kabul International Airport that took the life of an embassy local staff member.<sup>2</sup>

Notwithstanding the steps the Department has taken to improve security since the September 2012 attack on the U.S. Special Mission in Benghazi, Libya, OIG continues to find security deficiencies at a significant number of U.S. diplomatic facilities abroad.<sup>3</sup> Among the 27 U.S. diplomatic posts (“posts”

includes both embassies and their constituent posts) that OIG inspected in FY 2015, 18 were found to have physical security deficiencies at mission facilities or official residences. While some of these deficiencies were due to mission growth and the lack of sufficient work space in protected areas, many resulted from long-standing vulnerabilities that have not been addressed due to limited funds or mismanagement. While a process exists for seeking waivers or exceptions where security standards cannot be met, none of the OIG-identified security deficiencies had valid waivers or exceptions.

During FY 2015, OIG issued four reports related to the Accountability Review Board (ARB) report<sup>4</sup> on the Benghazi attack. The *Compliance Follow-up Review of the Special Review of the Accountability Review Board Process*<sup>5</sup> included one re-issued recommendation, which calls for the Department to develop minimum security standards that must be met prior to occupying facilities in Department-designated high-threat, high-risk locations. Additionally, a classified *Review of the Implementation of the Benghazi Accountability Review Board Recommendations*<sup>6</sup> examined the current state of implementation of the 29 recommendations from the classified ARB report. OIG concluded the Department completed the implementation of 13 recommendations; implementation was ongoing for ten and open-ended for six.

Two other OIG reports grew out of recommendations in the ARB report. After Benghazi, the Department developed an annual risk assessment process – the vital presence validation process (VP2) – under which senior Department officials assess whether posts in high-threat, high-risk locations

<sup>1</sup> Public Law No. 106-531, 114 Stat. 2537 (2000).

<sup>2</sup> Department of State, Bureau of Diplomatic Security, *2014 Year in Review – Finding the Balance*.

<sup>3</sup> All of the reports are classified.

<sup>4</sup> Department of State, *Accountability Review Board Report* (December 2014).

<sup>5</sup> OIG, *Compliance Follow-up Review of the Special Review of the Accountability Review Board Process* (ISP-C-15-33, August 2015).

<sup>6</sup> OIG, *Review of the Implementation of the Benghazi Accountability Review Board Recommendations* (ISP-S-15-34, August 2015).

should be opened, closed, or re-opened, and whether staffing levels are appropriate. In FY 2015, OIG reviewed VP2<sup>7</sup> and concluded it met the intent of the ARB recommendation and included information related to defining and prioritizing missions, assessing the risks and costs, explicitly identifying the risks and costs that cannot be mitigated, and having discussions on the need for constant attention to changes in the situation. However, VP2 did not explicitly address the ARB recommendation that such a process also assess the attainability of the posts' missions or the likelihood of the posts' achieving goals. Following up on another of the recommendations of the ARB, OIG conducted a special review of the storage at overseas facilities of fire accelerants and other weapons of opportunity and made recommendations to help better ensure their proper storage.<sup>8</sup>

During FY 2015, OIG found security deficiencies at residences of overseas personnel.<sup>9</sup> These deficiencies occurred for reasons that included the following: the Bureau of Diplomatic Security did not notify posts about substantial revisions to the Department's residential security program requirements in a timely manner and Regional Security Officers lacked sufficient understanding of these requirements and did not provide adequate oversight of post-specific residential security programs.

OIG also found weaknesses in emergency action planning at overseas posts. In a series of audits and management alerts on emergency action planning and responses at high-threat overseas posts, OIG found that posts generally had developed, and the Department had approved, plans for responding to emergency situations. However, not all posts routinely trained staff on the plans or practiced responding to potential emergencies as required. In addition, neither the posts nor the responsible bureaus ensured that posts had sufficient resources to respond to all types of emergencies or prolonged periods of crisis.<sup>10</sup> The failure to properly plan and practice emergency responses hampered the posts' responses to emergencies at high-threat posts, thereby increasing the potential for harm

to U.S. Government employees and facilities and the loss of critical information.

## 2 MANAGING POSTS AND PROGRAMS IN CONFLICT AREAS

The Department faces major challenges in responding to a broadening range of security and humanitarian crises in conflict zones. As of December 2014, more than 900 Foreign Service positions overseas were designated as unaccompanied tours of duty. On February 11, 2015, the Department suspended operations at Embassy Sana'a, Yemen, amid deteriorating security conditions. 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 2016 congressional budget justification requested \$7 billion in Overseas Contingency Operations funds to address the rise of the Islamic State in Iraq and the Levant, among other emerging challenges. The Department also expended \$3.05 billion in FY 2014 Migration and Refugee Assistance funds to respond to humanitarian crises.

Recognizing that managing posts and programs in conflict areas remains a challenge for the Department, OIG continued its series of audits examining the complex issue of providing security for embassy personnel. During FY 2015, OIG examined a contract awarded to Aegis Defense Services (Aegis) for security support at Embassy Kabul. Awarded as Task Order 10 under the Worldwide Protective Services (WPS) contract, the task order had cost the Department \$224 million at the time of the audit report's publication.<sup>11</sup> In the audit report, OIG found that the Department did not ensure that Aegis maintained records documenting contract-required training and security screening for employees working on the task order or time-and-attendance records to ensure that labor services billed to the U.S. Government were properly supported. OIG also found that invoices approved by the Contracting Officer's Representative contained more than \$8.6 million

<sup>7</sup> OIG, *Audit of the Department of State Implementation of the Vital Presence Validation Process* (AUD-SI-15-37, August 2015).

<sup>8</sup> OIG, *Management Assistance Report – Importance of Securing Fire Accelerants and Similar Weapons of Opportunity* (ISP-S-15-06, January 2015).

<sup>9</sup> OIG, *Management Assistance Report: Residential Security Concerns at U.S. Embassy Ankara, Turkey* (AUD-CGI-15-38, July 2015); OIG, *Management Assistance Report: Residential Security Concerns at U.S. Embassy Manila, Philippines* (AUD-CGI-15-29, May 2015).

<sup>10</sup> OIG, *Audit of Emergency Action Plans for U.S. Mission Pakistan* (AUD-MERO-14-08, December 2013).

<sup>11</sup> OIG, *Audit of the Bureau of Diplomatic Security Worldwide Protective Services Contract Task Order 10, Kabul Embassy Security Force* (AUD-MERO-15-03, October 2014).

in questioned costs. With respect to the security support at Embassy Baghdad, OIG will audit WPS Task Order 3, awarded to SOC LLC; the report will be issued during the first quarter of 2016.

OIG found that management support platforms were under stress at a number of posts where security concerns and growing workloads often drive staffing decisions. At one post in the Middle East, OIG recommended the Department address these issues, as political circumstances had transformed a formerly mid-size embassy into a large, front-line operation.<sup>12</sup> OIG observed that growth in the management support staff had not kept pace with the substantial increase in mission staffing, resulting in the need for extensive overtime and workload-related stress. OIG concurred with the post's request for five additional U.S. management positions, as well as an increase in local support staff.

A contributing factor to the stress on management support platforms is the practice among some non-Department agencies of using a series of long-term temporary-duty personnel to fulfill duties at embassies. In recent years, OIG has found that these temporary-duty personnel may receive management support services from the embassy, but the Department is not fully recovering costs, as required by 6 FAH-5 H-360, "Official Visits and Temporary Duty (TDY)."

The turbulent conditions in and around conflict areas make appropriate management of resources more difficult. An audit<sup>13</sup> found that 26 armored vehicles from Embassy Tripoli, Libya, that embassy personnel had used to evacuate to Tunis, Tunisia, remained stored and unused at Embassy Tunis, which had no need for them. The excess vehicles, valued at approximately \$5 million, were left stored in a grass and dirt lot on the embassy compound. OIG recommended that Embassy Tunis, in coordination with the Bureau of Near Eastern Affairs and the Bureau of Diplomatic Security, develop and implement a plan to redistribute and use the vehicles.

OIG found weaknesses in the design and oversight of assistance programs to Department programs in Syria and Pakistan. In its audit of humanitarian assistance programs in response to the Syrian crisis,<sup>14</sup> OIG found that, with respect to some programs, the Bureau of Population, Refugees and Migration neither conducted adequate risk assessments prior to an award nor conducted post-award monitoring. OIG documented problems with both the programs' performance and financial monitoring. OIG also found that grants policy directives for monitoring assistance awards to public international organizations may have been confusing for Department staff, leading to uncertainty on the requirements to manage and oversee these awards. Similarly, an audit of non-lethal aid provided to address the Syrian crisis<sup>15</sup> found weaknesses in monitoring and oversight, leaving foreign assistance vulnerable to waste, fraud, and abuse.

An audit of the Bureau of International Narcotics and Law Enforcement Affairs (INL) police training program in Pakistan<sup>16</sup> found that INL could not show that its training program was meeting the goal of enhancing the professionalism of the Pakistani police or increasing the capability of the Pakistani police to maintain peace and security. Moreover, INL could not determine whether the equipment provided by the program improved the survivability, mobility, and communications capacity of the Pakistani police. The audit also found that only 29 of 68 planned infrastructure projects were completed on schedule and that far fewer Pakistani police were trained by the program than had originally been planned. As a result, OIG identified more than \$86 million in funds that could be reprogrammed for other uses.

### 3 MANAGEMENT OF CONTRACTS AND GRANTS (INCLUDING FOREIGN ASSISTANCE OVERSIGHT)

Each year since 2008, OIG has identified the Department's management of contracts and grants as a management challenge; this area continued to be a challenge in FY 2015.

<sup>12</sup> OIG, *Inspection of Embassy Amman, Jordan* (ISP-I-15-29A, June 2015).

<sup>13</sup> OIG, *Management Assistance Report: Embassy Tripoli Armored Vehicles Available for Redistribution and Use* (AUD-MERO-15-28, May 2015).

<sup>14</sup> OIG, *Audit of Department of State Humanitarian Assistance in Response to the Syrian Crisis* (AUD-MERO-15-22, March 2015).

<sup>15</sup> OIG, *Audit of Department of State's Management and Oversight of Non-Lethal Assistance to Address the Syrian Crisis* (AUD-MERO-15-39, September 2015).

<sup>16</sup> OIG, *Audit of the Bureau of International Narcotics and Law Enforcement Affairs Law Enforcement Reform Program in Pakistan* (AUD-MERO-15-04, October 2014).

## Contract Management

In March 2014, OIG issued a management alert on contract file deficiencies, noting repeated and widespread examples of poor contract file administration within the Department.<sup>17</sup> Despite that alert, inspection and audit teams continued to find problems, including the lack of annual procurement plans; incomplete files that lacked required documentation; and failure to properly designate, train, and certify Contracting Officer and Grants Officer Representatives (CORs and GORs).<sup>18</sup> In FY 2015, audits, inspections, and investigations placed heavy emphasis on these and other areas to which OIG attributed significant shortcomings identified in the administration and oversight of Department awards.

Examples of weaknesses in contract administration and oversight were included in a report on an audit of the New Embassy Compound in London,<sup>19</sup> which determined that the Contracting Officer did not obtain sufficient data when negotiating the final price for the construction portion of the contract. As a result, the contractor was not required to explain the approximately \$42 million difference between the initial proposal (submitted in 2012) and the final proposal (submitted in 2013). OIG concluded that improper price negotiations left the Department vulnerable to funds being wasted or misused.

OIG also audited the Aviation Support Services Contract in Iraq<sup>20</sup> and questioned costs of almost \$1 million that were not identified by the Department because of insufficient invoice review processes, methodologies, and staffing. The audit also questioned another \$25.9 million associated with employer and employee Iraqi personal income tax reimbursements approved by the Department. As a result of this audit, OIG recommended the Department review the questioned costs and made additional recommendations for improving contract management and oversight.

In addition, OIG audited the Medical Support Services Contract in Iraq<sup>21</sup> and found that the Department had only one COR to monitor all 15 task orders under the contract valued at \$1 billion. The lack of government oversight personnel is an issue frequently found in OIG's work. OIG issued both a management alert and an audit report expressing concerns that, in the absence of a COR, various embassy personnel were directing the contractor to perform work outside the scope of the contract. The report concluded that these actions exposed the Department to unauthorized commitments and claims made by contractors.

Contract closeout, which is the final phase in a contract's life cycle, is a key step in ensuring that the Department has received the appropriate goods and services at the agreed-upon price. During a review to determine whether the Department had effectively and efficiently closed out contracts supporting the U.S. Mission in Afghanistan,<sup>22</sup> OIG learned that the Department did not consistently meet government- and Department-wide contract management and closeout requirements for the 87 Afghanistan-related task orders included in OIG's review. Some of the issues identified included contract closeout timelines that were not being met for 32 percent of the contracts reviewed and contract files that were lost, prematurely destroyed, or incomplete. As a result, files for \$68 million in contracts could not be located or were prematurely destroyed, \$6.3 million in funding had not been de-obligated and had expired, and up to \$52 million in funding was available for de-obligation.

## Grant Management

The Department's ongoing challenge with the administration and oversight of grants was the subject of several OIG audits, including an audit of GORs that identified instances where GORs did not execute their oversight responsibilities or

<sup>17</sup> OIG, *Management Alert – Contract File Management Deficiencies* (MA-A-0002, March 2014).

<sup>18</sup> OIG, *Inspection of Embassy Antananarivo, Madagascar* (ISP-I-15-20A, May 2015).

<sup>19</sup> OIG, *Audit of the Construction Contract Award and Security Evaluation of the New Embassy Compound London* (AUD-CGI-15-31, July 2015).

<sup>20</sup> OIG, *Audit of the Bureau of International Narcotics and Law Enforcement Affairs Aviation Support Services Contract in Iraq* (AUD-MERO-15-35, July 2015).

<sup>21</sup> 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, *Management Assistance Report—Concerns With the Oversight of Medical Support Service Iraq Contract No. SAQMMA11D0073* (AUD-MERO-15-20, December 2014).

<sup>22</sup> OIG, *Audit of the Contract Closeout Process for Contracts Supporting the U.S. Mission in Afghanistan* (AUD-MERO-15-14, November 2014).

comply with grant monitoring requirements.<sup>23</sup> OIG also reported improprieties of one grantee,<sup>24</sup> including instances of non-adherence with Federal procurement requirements. In this report, OIG recommended the Department assess the allowability of more than \$1.5 million in payments made to the grantee.

In FY 2015, OIG inspections teams issued 35 formal recommendations to improve monitoring, justification for sole-source procurement, reporting, documentation, training, and overall grants management. In one inspection of a domestic bureau,<sup>25</sup> all 31 grant files inspected (totaling \$38 million) lacked monitoring plans. Twenty-three were sole-sourced and five of those did not contain the required justifications. The remaining 18 had poor justifications and cited an incorrect statutory authority for the sole-sourced procurement.

During an audit<sup>26</sup> of the National Endowment for Democracy (NED), OIG found that, from FY 2006 through FY 2014, the Department awarded more than \$963 million to NED but had not conducted required audits of NED financial transactions. Further, the terms and conditions of the annual grant to NED did not include the language related to the audit requirement. OIG also found that the Department did not comply with other requirements for monitoring NED, including reconciling submitted financial reports with the grant awards and maintaining sufficient grant files. OIG recommended the Department conduct required audits of NED financial transactions and amend its grant agreement with NED to include the terms of the audit requirement in order to decrease the risk that funds dedicated to promoting democracy were misapplied.

Grants management was specifically a challenge for Public Diplomacy Officers at embassies. OIG identified grant management deficiencies in 8 of the 11 Public Affairs Sections at overseas missions inspected in FY 2015. The most

common deficiencies were lack of documentation or failure to enter timely information in the database management system and lack of monitoring activities, which created uncertainty about the status of the grants and made it difficult to document the completion and closeout of the grants. Further deficiencies include the absence of trained and accredited grants management personnel, resulting in the inability to provide accountability for proper disbursements and program evaluations.

An audit of the Export Control and Border Security (EXBS) program<sup>27</sup> found that headquarters personnel did not adequately administer and oversee foreign assistance funding dedicated to certain EXBS programs. As a result, headquarters personnel could not ensure that the award's purposes were being achieved, and they could not demonstrate that they had safeguarded the integrity of funds or reduced financial risk to the EXBS program. OIG recommended that the Department's Office of Export Control Cooperation establish and implement a process to monitor contractor and grantee files, improve award administration and oversight, establish and maintain program files, and conduct end-use monitoring. Similar issues were identified in the audit of the Global Threat Reduction program.<sup>28</sup>

#### 4 INFORMATION SECURITY AND MANAGEMENT

The Department spent about \$1.4 billion on information technology in FY 2015. The same year, a number of cybersecurity incidents illustrated deficiencies in the Department's efforts to protect its computer networks. Malicious actors exploited vulnerabilities, causing potential compromise of sensitive information and significant downtime to normal business operations.

In 25 overseas and domestic inspections conducted from May 2014 through June 2015, OIG found 37 shortcomings

<sup>23</sup> OIG, *Audit of Department of State Oversight Responsibilities, Selection, and Training of Grants Officer Representatives* (AUD-CG-15-33, June 2015).

<sup>24</sup> OIG, *Management Assistance Report—Grant Improprieties by Nour International Relief Aid* (AUD-CG-15-19, January 2015).

<sup>25</sup> OIG, *Inspection of the Bureau of Political-Military Affairs* (ISP-I-15-27, June 2015).

<sup>26</sup> OIG, *Management Assistance Report: Oversight of Grants to the National Endowment for Democracy* (AUD-SI-15-34, June 2015).

<sup>27</sup> OIG, *Audit of Bureau of International Security and Nonproliferation Administration and Oversight of Foreign Assistance Funds Related to the Export Control and Related Border Security Program* (AUD-SI-15-23, April 2015).

<sup>28</sup> OIG, *Audit of the Bureau of International Security and Nonproliferation Administration and Oversight of Foreign Assistance Funds Related to the Global Threat Reduction Program* (AUD-SI-15-41, September 2015).

in cybersecurity, concerning issues including access controls, configuration management, and encryption. Inadequate performance of information systems security officer (ISSO) duties was the most common finding; OIG found poor or inconsistent performance of ISSO duties in 10 of 25 inspections. ISSO responsibilities include reviewing event logs, randomly checking user libraries, and reminding users of security awareness. Failure to carry out these tasks can leave a system vulnerable to a wide range of threats, such as spear-phishing attacks. Many of the cybersecurity findings were remedied during the inspections and OIG issued 18 recommendations to address remaining weaknesses.

The Department also continues to face difficulties meeting the requirements of the FISMA and implementing a fully effective information security management program. During the FY 2014 FISMA audit,<sup>29</sup> OIG identified security control weaknesses that had significantly affected the information security program, potentially undermining the confidentiality, integrity, and availability of information and information systems. Because these serious vulnerabilities have recurred for several years, OIG considers the collective security weaknesses a significant deficiency under FISMA.<sup>30</sup>

OIG also reported<sup>31</sup> that the Department did not organize and successfully implement Active Directory Rights Management, which is necessary to enforce IT security standards. Specifically, OIG identified deficiencies in the Bureau of Information Resource Management's oversight of the management of user accounts that allowed thousands of unused accounts to remain active, posing a significant risk for unauthorized access and use, as well as unnecessary maintenance costs. OIG made 33 recommendations to address issues raised in the audit. In addition, OIG identified significant program challenges with the Department's security program for wireless networks<sup>32</sup> and made three recommendations to the Department to strengthen its wireless program.

Information technology contingency planning, which has been a recurring subject of OIG inspection reports and was the subject of a 2011 special memorandum report,<sup>33</sup> continues to be a management challenge for the Department. In 19 inspections conducted in FY 2015, OIG identified deficiencies in contingency planning, including the complete lack of a contingency plan, the failure to test the plan, and poor implementation of a plan during an actual emergency event. Instability in many regions of the world and recent attacks and threats against the Department's personnel and diplomatic facilities demonstrate the need for contingency planning and readiness to respond to crisis situations in order to maintain communications and continuity of business operations.

OIG also identified weaknesses in the Department's implementation of its "record email" technology that adversely affect its core mission of conducting the foreign relations of the United States as well as its records retention responsibilities. In 2009, the Department implemented "record email" to facilitate the preservation of records contained in emails. However, inspection reports issued over several years have noted widespread use of ordinary Department email, which is not distributed widely and is not retrievable for reporting and other purposes related to policy-making and implementation. An FY 2015 OIG inspection<sup>34</sup> found that the Bureau of Administration does not review record email use across bureaus or missions and noted that Department employees have not received adequate training or guidance on their responsibilities for using record emails to meet records retention responsibilities.

### Vulnerabilities in Consular IT Systems

The Bureau of Consular Affairs' (CA) Consular Consolidated Database (CCD) experienced major system failures in the busy summer seasons of both 2014 and 2015. This unreliability undermines CA's ability to provide consular services that protect U.S. citizens abroad and facilitate the entry of

<sup>29</sup> OIG, *Audit of the Department of State Information Security Program* (AUD-IT-15-17, November 2014).

<sup>30</sup> OIG, *Management Alert: OIG Findings of Significant and Recurring Weaknesses in the Department of State Information System Security Program* (MA-A-0001, January 2013).

<sup>31</sup> OIG, *Audit of the Department of State Implementation and Oversight of Active Directory* (AUD-IT-15-05, October 2014).

<sup>32</sup> OIG, *Management Assistance Report: Department of State Security Program for Wireless Networks* (AUD-IT-15-27, May 2015).

<sup>33</sup> OIG, *Memorandum Report – Improvements Needed in Information Technology Contingency Planning* (ISP-I-12-04, December 2011).

<sup>34</sup> OIG, *Review of State Messaging and Archive Retrieval Toolset and Record Email* (ISP-I-15-15, March 2015).

legitimate foreign visitors and immigrants, while ensuring U.S. border security. In FY 2014, CA issued 14.1 million passports and passport cards to U.S. citizens, as well as nearly 10 million non-immigrant visas and more than 467,000 immigrant visas.<sup>35</sup> CA operations depend on the CCD to store visa and passport applications; perform required security checks; issue the final products (visas and U.S. passports); and ensure the utility, reliability, and integrity of the process. Other U.S. Government agencies also rely on the CCD.

In July 2014, problems with the CCD temporarily prevented issuance of visas to visitors and immigrants as well as issuance of U.S. passports. A larger system failure occurred from May 29 through July 6, 2015, resulting in backlogs in the issuance of immigrant visas, nonimmigrant visas, and overseas U.S. emergency passports. CA is in the process of upgrading hardware and modernizing the various databases that make up the CCD and is planning to launch a new system to replace the current CCD. OIG will continue to monitor CA's progress and will inspect CA's Office of Consular Systems and Technology in the spring of 2016.

## 5 FINANCIAL MANAGEMENT

Financial management continues to be a significant management challenge for the Department. During the audit of the FY 2014 financial statements,<sup>36</sup> an independent external auditor identified significant internal control deficiencies related to financial reporting, property and equipment, budgetary accounting, unliquidated obligations, and information technology. Total FY 2014 obligations for the Department consisted of contractual services of \$14.7 billion, grants and fixed charges of \$16.7 billion, and acquisition of assets of \$2.8 billion, which collectively represented 79 percent of the agency's spending.<sup>37</sup>

Providing adequate oversight and coordination of foreign assistance resources also remains a challenge for the Department. A systemic problem hindering effective coordination and oversight is the Department's financial management systems, which were not designed to track and report on foreign assistance funds. As reported in a management assistance report,<sup>38</sup> the Department's core financial systems do not track foreign assistance funding and expenditures by program, project, country, region, or purpose (sector), even though Department and individual bureaus need this information to track and manage their foreign assistance funds and respond to external queries. Department bureaus with foreign assistance funds have spent millions of dollars and an inordinate amount of time, with limited success, on alternative systems and processes to fill this gap.

<sup>35</sup> Department of State, Bureau of Consular Affairs, *Functional Bureau Strategy 2015-2017*.

<sup>36</sup> OIG, *Independent Auditor's Report on the U.S. Department of State 2014 and 2013 Financial Statements* (AUD-FM-15-07, November 2014).

<sup>37</sup> Department of State, *Fiscal Year 2014 Agency Financial Report* (November 2014).

<sup>38</sup> OIG, *Management Assistance Report – Department Financial Systems Are Insufficient to Track and Report on Foreign Assistance Funds* (ISP-I-15-14, March 2015).

# Management's Response to Inspector General

In 2015, the Department of State's Office of Inspector General (OIG) identified management and performance challenges in the areas of: protection of people and facilities; managing posts and programs in conflict areas; management of contracts and grants; information security and management; and financial management. The Department promptly takes corrective actions in response to OIG findings and recommendations. Highlights are summarized below.

1. PROTECTION OF PEOPLE AND FACILITIES	
<b>Challenge Summary</b>	Protecting overseas personnel and facilities continues to be a major management challenge for the Department.
<b>Actions Taken</b>	<p><b>Vetting Local Guards:</b> The Bureau of Diplomatic Security (DS) developed the Security Officer Collective to advise Regional Security Officers who serve as Contracting Officer Representatives on the importance of implementing oversight of guard force contracts and vetting contract guards as well as the new templates to use during the process. The Department's Local Guard Program Handbook that addresses this requirement is expected to be published early 2016.</p> <p><b>Physical Security Standards:</b> DS modified and improved the new physical security survey templates. DS has also launched a Deficiencies Database to comprehensively identify all physical security deficiencies and manage them until they are resolved. When the Database is fully populated with deficiencies for all overseas facilities – anticipated for September 2016 – it will be used to assist the Bureau of Overseas Buildings Operations (OBO) in the prioritization of physical security upgrade funding using quantitative risk scores. DS also worked with OBO to update the Physical Security Handbook to clarify requirements for Safe Havens and Safe Areas.</p> <p><b>Physical Security Upgrades, Worldwide:</b> To address deficiencies, DS undertook numerous physical security projects at posts. Further classified details are available.</p> <p><b>Armored Vehicles:</b> DS worked with the Bureau of Near Eastern Affairs to address the relocation of vehicles from Libya to Tunis, Tunisia. Additionally, DS reviewed the armored vehicle driver training requirements and determined Embassy Tunis had a requirement to train approximately 17 armored vehicle drivers. The Training Directorate in DS is planning to send instructors to Tunisia to conduct armored vehicle training.</p> <p><b>Emergency Action Planning:</b> DS updated its Emergency Planning Handbook to reflect its established process to validate by physical inspection those supplies and resources identified in the Emergency Action Plan (EAP) are present and appropriate for each type of contingency. DS has begun updating the Post Security Program Review Compliance Rating Form to capture EAP validation requirements.</p> <p><b>Marine Security Guard Program:</b> DS reviewed and updated the Memorandum of Agreement between the Department and the U.S. Marine Corps (USMC) for the Operational and Administrative Supervision of the Marine Security Guard Program to reflect the expansion of the Program. DS completed revisions to Annexes D and J and are negotiating edits with the USMC.</p>
<b>Actions Remaining</b>	<p><b>Vetting Local Guards:</b> DS has revised the Local Guard Program Handbook and the revisions are in the DS clearance process. Once cleared, the handbook will go through Department clearance.</p> <p><b>Physical Security Standards:</b> The subchapter, Safe Havens, Safe Areas, and Compound Emergency Sanctuaries, in the Physical Security Handbook is currently in the DS clearance process. Once cleared, the subchapter will go through Department clearance.</p>

2. MANAGING POSTS AND PROGRAMS IN CONFLICT AREAS	
<b>Challenge Summary</b>	The Department faces major challenges in responding to a broadening range of security and humanitarian crises in conflict zones.
<b>Actions Taken</b>	From the Post Management perspective, most of our challenges relate to Government of Pakistan (GoP) bureaucracy. The GoP limits the size and weight of incoming secure pouches, causing a backlog of courier-escorted shipments of classified material and CAA items, routinely 8-12 months. The inability to obtain No Objections Certificates for the GoP substantially encumbers the Mission's ability to expand its telecommunications circuits/capabilities in country. GoP bureaucracy in both the Ministry of Foreign Affairs and the Customs Bureau causes delays in importation and export of both personal effects and official goods, including fully-armored vehicles which are limited to a strict quota based on the number of permanent positions and thus too few to support all needs. These bureaucratic complexities extend to visa issuance, which in some cases can take three to six months and more, and have caused numerous instances of hardship to travelers and major delays for a broad array of projects and programs.
<b>Actions Remaining</b>	The Department is actively working to implement the OIG recommendations, including negotiating a new Letter of Agreement for the assistance to Pakistan for 2016, and updating the financial management handbook. The Department continues to work with the OIG on its remaining recommendations, and will issue new guidance for advances and related controls.
3. MANAGEMENT OF CONTRACTS AND GRANTS	
<b>Challenge Summary</b>	Each year since 2008, OIG has identified the Department's management of contracts and grants as a management challenge; this area continued to be a challenge in FY 2015.
<b>Actions Taken</b>	<p>The complex portfolio of contract and grant programs performed around the globe present significant management challenges that continue to be addressed through partnership with OIG, policies, training, and oversight.</p> <ul style="list-style-type: none"> <li>■ More detailed policies, guidance, and training were issued to strengthen contract files in response to OIG recommendations. The Department created an audit program and identified additional resources to review contract files. The Department is developing and deploying electronic files to improve compliance.</li> <li>■ The Department issued guidance on use of the contract type used in the New Embassy Compound in London to ensure proper contract administration.</li> <li>■ As recommended by the OIG, the Department reviewed questioned costs under the Aviation Support Services Contract in Iraq and provided OIG rationale for reasonableness of decisions made.</li> <li>■ Additional Contracting Officer Representatives (CORs) were assigned to monitor the Medical Support Services Contract in Iraq. This significant contract undertaking successfully transferred medical responsibilities from DoD to the Department of State within tight transition timelines. A Contract Management Office was created to ensure continuity because of rotation of personnel in this challenging environment.</li> <li>■ Detailed contract closure guidance was issued to improve contract closure.</li> <li>■ As noted by the GAO, GAO-14-635, the Department of State has a robust policy infrastructure for the administration of grants.</li> <li>■ A Grants Officer Representative (GOR) program was instituted to train and certify GORs to monitor grants. Over 1,200 GORs have now been certified. No other agency is known to have a similar program.</li> <li>■ Training for GORs and Grants Officers has been updated and expanded. Special training in new Government-wide grants regulations resulted in the Department of State being the first agency to deploy new regulations. Other agencies are examining the Department's training.</li> <li>■ The Department completed a Grants Human Capital Plan to better manage grant operations resources. Similar plans have not been found at other agencies.</li> <li>■ As recommended by the OIG, the Department initiated audits of the National Endowment for Democracy and amended its grant agreement to provide for future audits.</li> <li>■ Grants policies address grant monitor and risk assessment. The Department continues to expand training in this important topic.</li> </ul> <p>Individual program offices continue to work with the OIG to resolve specific audit recommendations.</p>
<b>Actions Remaining</b>	<ul style="list-style-type: none"> <li>■ Provide documentation to the OIG to close out recommendations.</li> <li>■ Provide continuous training to ensure competent CORs and GORs.</li> </ul>

**4. INFORMATION SECURITY AND MANAGEMENT**

<b>Challenge Summary</b>	The Department spent approximately \$1.4 billion on information technology worldwide in FY 2015. The same year, the Department faced a cybersecurity incident that impacted the Department's ability to protect its computer networks. Malicious actors used a combination of undisclosed computer application vulnerabilities and Department network weaknesses to access systems. The Department's response necessitated downtime to Internet access.
<b>Actions Taken</b>	The Department experiences numerous, repeated attempts to gain unauthorized access to its unclassified network annually. In 2015, an attempt by a sophisticated malicious actor was successful. The Department coordinated with cybersecurity experts from the Federal Government and private industry to detect and expel this intrusion. As a result of this unauthorized intrusion, and the efforts undertaken to restore and recover from the event, the Department has evaluated and moved aggressively to install new cybersecurity capabilities to enhance protection and detection. These enhancements are being applied with the most likely targets being addressed first. In addition, the Department of State is following the Department of Homeland Security's operational directive to resolve all identified critical and high rated weaknesses in its Internet facing systems that are identified through routine weekly scans.
<b>Actions Remaining</b>	In addition to the solutions deployed, the Department is actively moving to implement a network architecture that is more resilient. These actions, coupled with the Office of Management and Budget Cyber Sprint and Cross-Agency Priority Goals and Department of Homeland Security's Continuous Diagnostics and Mitigation program capabilities, will strengthen the Department's resilience and cybersecurity situation awareness to act where needed.

**5. FINANCIAL MANAGEMENT**

<b>Challenge Summary</b>	Financial Management continues to be a significant management challenge for the Department.
<b>Actions Taken</b>	The Department received a clean ("unmodified") opinion from the external Independent Auditor on our 2014 Department-wide financial statements, including no reported material weaknesses in internal controls. In 2015, the Department sustained efforts to address and reduce weaknesses in financial reporting, property and equipment, budgetary accounting, unliquidated obligations, and information technology. For example, bureaus are taking significant efforts to manage unliquidated obligations and we have reduced the extent of manual processes in our preparation of financial statements. In addition, the Department implemented the Governmentwide Treasury Account Symbol Adjusted Trial Balance System (GTAS) as the primary means of reporting agency trial balance data to the Department of the Treasury. The Independent Auditor continues to provide an unmodified or "clean" opinion on our financial statements, clear of any material weaknesses. The Department conducted its assessment of internal controls over financial reporting in accordance with OMB Circular A-123 Appendix A and found them to be operating effectively resulting in an unqualified statement of assurance. We continue to bolster the Department's improper payments and recapture audit program, and in their 2014 annual assessment, the OIG found the Department's improper payments program to be in substantial compliance with IPIA.
<b>Actions Remaining</b>	The Department will continue efforts to address weaknesses in financial reporting, property and equipment, budgetary accounting, unliquidated obligations, and information technology.