

that they were) testing IT contingency plans annually.⁵⁹ For example, OIG found that Embassy Tel Aviv in Israel had not updated its plan annually, which, in turn, meant that managers did not provide initial and annual refresher contingency training to information management personnel.⁶⁰ The lack of a properly developed and tested IT contingency plan that is linked with overall emergency preparedness processes could compromise a post's recovery efforts following an IT incident. OIG has accordingly recommended repeatedly that overseas posts conduct IT contingency planning in accordance with Department standards.

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

Establishing Effective Records Management Programs

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

in which it observed safes containing classified documents from departed employees that were not retired, archived, or disposed.⁶⁵

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

4 FINANCIAL AND PROPERTY MANAGEMENT

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

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

⁶⁰ ISP-I-17-20, May 2017.

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

⁶² ISP-I-17-22, May 2017.

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

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

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