managers to ensure compliance with information systems security standards. In a management assistance report, OIG reported that one third of its overseas inspections conducted from fall FY 2014 to spring FY 2016 included findings related to the deficient performance of ISSO duties.[53] Similarly, several FY 2017 inspections confirmed that this continued to be a problem for the Department both at overseas posts and domestic bureaus.[54]

Because ISSO duties are often assigned to information management personnel on a collateral basis, competing priorities are sometimes at the root of this challenge. Neglect of these duties, however, may leave the Department vulnerable to cybersecurity attacks. Accordingly, OIG recommended that the Bureau of Information Resource Management (IRM) take the lead in implementing a plan to enforce the performance of ISSO duties by overseas information management personnel in accordance with Department standards.[55] Additionally, OIG issued recommendations for individual overseas posts to implement standard operating procedures to ensure performance of ISSO duties.

OIG also found missed opportunities to improve systems through use of the Department's cybersecurity assessment reports. These reports, which are conducted by DS, focus on cybersecurity practices and include specific recommendations for improvement. In comparing its own reports with DS reports, OIG found that, of the 23 instances in which DS performed a cybersecurity assessment before an OIG inspection of a post, subsequent OIG reports made recommendations reflecting the same or similar deficiencies 18 times.[56] The specific recommendations related to a range of issues, including inadequate performance of ISSO duties, incomplete or untested IT contingency plans, unidentified dedicated internet networks, physical control deficiencies, administrative control weaknesses, and technical control issues. To address this serious issue and to ensure that the Department is taking advantage of its own processes to protect its information security, OIG recommended that the Department require implementation of cybersecurity assessment recommendations and establish a process to track and verify compliance.[57]

Another report on this subject detailed concerns with the Department's configuration change control process. Configuration change control prevents changes to IT systems or changes that could introduce security weaknesses—such system changes can be as minor as adding a new type of printer or as significant as deploying an entirely new application.[58] At the Department, enterprise change requests must be reviewed through a process led by the Information Technology Configuration Control Board. OIG reported that this board did not authorize or test change requests in compliance with Federal requirements and Department policy. Specifically, change requests were not sufficiently authorized at every stage of the review process, and change requests were not tested as required. As a result of unauthorized and untested change requests, the Department's network, applications, and software are put at risk because of an inconsistently applied and controlled configuration control process.

OIG also continued to find deficiencies in Department IT contingency planning at overseas posts. Department guidelines require every information system to have a contingency plan that is documented and tested annually. Incomplete and untested IT contingency plans increase the risk of ineffective responses to or loss of critical communication during an emergency or crisis. OIG found several embassies that were not (or could not show

---

53 OIG, *Management Assistance Report: Non-Performance of Information Systems Security Officer Duties by Overseas Personnel* (ISP-17-24, May 2017).

54 OIG, *Inspection of Consulate General Jerusalem* (ISP-I-17-18, June 2017); ISP-I-17-12, May 2017; ISP-I-17-16, May 2017; ISP-I-17-20, May 2017; ISP-I-17-13, ISP-I-17-22, May 2017, March 2017.

55 ISP-17-24, May 2017.

56 OIG, *Management Assistance Report: Deficiencies Reported in Cyber Security Assessment Reports Remain Uncorrected* (ISP-17-39, July 2017). The DS assessments occurred between 1 and 41 months before OIG's inspection, with an average of over 10 months between the two reports.

57 *Ibid*.

58 OIG, *Audit of the Department of State's Information Technology Configuration Control Board* (AUD-IT-17-64, September 2017).