- The Enterprise Risk Officer for Cybersecurity coordinated the response to EO 13800 Section 1 which was submitted in accordance with OMB Memorandum-17-25, *Reporting Guidance for Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure.*
- The Department reduced the backlog of pending security assessments by assessing and authorizing 28 percent of that backlog of systems during 2017.

Protect

- The Department significantly reduced the number of stale accounts (accounts not logged into in the last 90 days) and misconfigured accounts (i.e., shared mailboxes not configured to use SmartCards) on the Department's network in order to improve access controls.
- The Department deployed a phishing awareness tool and quarterly exercises that test and train employees how to recognize and correctly respond to phishing attacks to provide enterprise-wide awareness on how to identify and avoid phishing threats.

Detect

- The Department continues to leverage the Department of Homeland Security's Continuous Diagnostics and Mitigation (CDM) Program. The CDM Program enhances our existing tools to ensure all hosts, regardless of operating system, are identified and monitored for vulnerabilities.
- The Department implemented the first phase of CDM including hardware and software identification.
- The Department deployed cyber detection dashboards to aggregate server logs in an effort to quickly identify anomalies on the network.
- The Department conducted penetration tests by both internal and external partners.

Response

- The Department established the Cybersecurity Integrity Center, under the Joint Security Operation Center concept, to further enhance cyber monitoring activities and the Department's ability to detect anomalous behavior on the network.
- The Department is updating the Joint Security Operation Center's Incident Response Plan with clear roles and responsibilities.

Recover

- The Department established High Availability/Disaster Recovery for critical functions.
- The Department updated and tested the annual Contingency Plan (CP) tests following the recent changes to the accredited cybersecurity posture. The Department's CP assessments will continue to be reviewed as needed.

In its FY 2017 FISMA Report, the OIG cites significant weaknesses to information systems security. The Department acknowledges the weaknesses identified by the OIG in its FISMA review but does not believe that any of the FISMA findings, either individually or collectively, rise to the level that requires reporting of a material weakness under FMFIA. The Department of State remains committed to adopting the best cybersecurity practices and embedding them into the Department's culture. As a result, we continue to improve our cybersecurity posture and provide transparency across the Department and with external partners.

Other Regulatory Requirements

The Department is required to comply with a number of other legal and regulatory financial requirements, including the Improper Payment Information Act (IPIA, as amended), the Debt Collection Improvement Act, and the Prompt Payment Act. The Department determined that none of its programs are risk-susceptible for making significant improper payments at or above the threshold levels set by OMB. In addition, the Department does not refer a substantial amount of debts to Treasury for collection, and has successfully paid vendors timely over 97 percent of the time for the past three fiscal years. A detailed description of these compliance results and improvements is presented in the Other Information section of this report.