Report in Brief

AUGUST 4, 2016

Why We Did This Review

The Cybersecurity Act of 2015 (the Act) requires that each office of inspector general (OIG) submit a report to Congress on the national security systems and systems that provide access to personally identifiable information (PII) operated by or on behalf of its department.

The Act requires the report to include the following areas: logical access policies and practices and logical access controls, multi-factor authentication, software inventory policies and procedures, capabilities to monitor and detect exfiltration and other threats, and policies and procedures that ensure contractors' implementation of information security management practices.

Objective and Scope

The objective of this audit is to examine the IT security policies, procedures, practices, and capabilities—as defined in the Cybersecurity Act of 2015—for national security and PII systems.

While the Secretary of Commerce is ultimately responsible for ensuring the security of the Department's information and information systems, senior officials must manage and supervise the IT security programs in their respective operating units (OUs). For this reason, we examined both the Department and the individual OU IT security policies, procedures, practices, and capabilities.

There are 146 systems that provide access to PII managed by 9 of the 13 OUs within the Department. To conduct our work, we collected and reviewed information on the five areas specified in the Act from each of the 9 OUs: Bureau of Industry and Security (BIS), Census Bureau (Census), International Trade Administration (ITA), National Institute of Standards and Technology (NIST), National Oceanic and Atmospheric Administration (NOAA), National Telecommunications and Information Administration (NTIA), National Technical Information Service (NTIS), Office of the Secretary (OS), and U.S. Patent and Trademark Office (USPTO).

OFFICE OF THE SECRETARY

Review of IT Security Policies, Procedures, Practices, and Capabilities in Accordance with the Cybersecurity Act of 2015

OIG-16-040-A

RESULTS ON PII SYSTEMS

We have provided the required descriptions for each of the five areas specified in the Act by identifying common attributes of the IT security policies, procedures, practices, and capabilities across the 9 OUs.

I. *Logical access policies and practices and logical access controls.* In general, logical access policies and practices used by the Department follow appropriate standards, and OUs have asserted logical access controls are in place on most systems. However, we found that NOAA and OS had outdated policies, and Census and USPTO had not fully implemented logical access controls on their systems. More specifically, we found that logical access controls for 10 of the 12 Census systems and 1 of the 4 USPTO systems selected for review were not fully implemented. Census and USPTO developed plans of action and milestones to address the weaknesses identified. As of June 2016, Census has completed the needed corrective actions, and USPTO anticipates completing corrective actions by September 2016.

II. *Multi-factor authentication.* The Act directs OIG to (a) list and describe the multi-factor authentication used by the Department to govern privileged users' access to systems and (b) describe any reasons for not using multi-factor authentication. Our review identified that 5 of the 9 OUs—Census, NIST, NOAA, OS, and USPTO—have not fully implemented multi-factor authentication for privileged users on PII systems.

III. *Software inventory policies and procedures.* The Act directs OIG to describe the policies and procedures followed by the Department to conduct inventories of the software present on the systems. The Department's policy requires that OUs maintain asset inventories for network-connected IT devices, including system software release information. All 9 OUs implement procedures to conduct inventories of the software present on the systems.

IV. *Capabilities to monitor and detect exfiltration and other threats.* The Act directs OIG to describe (a) what capabilities the Department utilizes to monitor and detect exfiltration and other threats, (b) how it is using them, and (c) any reasons for not utilizing such capabilities. We found that all 9 OUs deploy the following capabilities to monitor and detect exfiltration and other threats: external monitoring, security operations centers, intrusion detection systems/intrusion prevention systems, and event correlation tools.

V. *Policies and procedures that ensure contractors' implementation of information security management practices.* The Act directs OIG to describe the policies and procedures of the Department ensuring that contractors are implementing the information security management practices. Contractors that provide IT services to the Department are required to follow the Department's IT Security Program Policy, which specifically requires information system monitoring and software management. Further, the Department requires the IT Compliance in Acquisition Checklist be completed for information system acquisitions.

FINDINGS AND RECOMMENDATIONS

Appendix B, "National Security Systems," presents the results of our review of the Department's national security systems in accordance with the Act. The results, findings, and recommendations contained in appendix B are for official use only.