Report in Brief

March 22, 2023

Background

The U.S. Department of Commerce (the Department) and its bureaus are required to follow federal laws to secure information technology (IT) systems through the cost-effective use of managerial, operational, and technical controls. This responsibility applies to all IT systems, including those from the Office of the Secretary (OS), which serves as the general management arm of the Department and provides principal support to the Secretary in formulating policy and providing advice to the President. The Office of the Chief Information Officer (OCIO) is responsible for managing OS' information systems and applications.

At the Department, OS and many other bureaus operate independent Security Operations Centers (SOCs), which are responsible for detecting and responding to cybersecurity incidents. OS' SOC (OS SOC) within OCIO manages day-to-day IT security operations. Additionally, the Department has established a separate Enterprise SOC (ESOC) that manages the Department's network perimeter, compiles data from bureau SOCs, and serves as a liaison to government cybersecurity partners such as the Cybersecurity & Infrastructure Security Agency.

Why We Did This Review

Our evaluation objective was to assess the adequacy of actions taken by the Department and its bureaus when detecting and responding to cyber incidents in accordance with federal and Departmental requirements.

OFFICE OF THE SECRETARY

Fundamental Deficiencies in OS' Cybersecurity Incident Response Program Increase the Risk of Cyberattacks

OIG-23-017-I

WE FOUND the following:

I. OS SOC's security tools were not properly configured to detect incidents.

II. OS SOC did not effectively handle a simulated incident.

III. OS OCIO did not manage its incident detection and response program in accordance with federal requirements.

WE RECOMMENDED that the Deputy Secretary of Commerce direct the Department's Chief Information Officer to do the following:

1. Perform a review of all software tools used within OS to ensure that default passwords are not used.
2. Ensure that OS OCIO holds its contractors accountable for implementing Department policy on default passwords.
3. Establish a process to regularly review OS SOC tools and ensure they are configured correctly and operating as intended.
4. Review and revise OS OCIO firewall configurations and rulesets to ensure that they are providing adequate protection to OS systems.
5. Establish processes and procedures to periodically review OS OCIO firewall configurations and rulesets.
6. Obtain the capability for OS OCIO to automatically aggregate security events and data using a tool such as Security Information and Event Management.
7. Review OS's Data Loss Prevention practices, including but not limited to updating the configurations of Data Loss Prevention products and ensuring that incidents are reported to OS SOC and ESOC in a timely manner.
8. Update the existing service-level agreement to define clear responsibilities between ESOC and OS for the incident handling process.
9. Update OS OCIO's cybersecurity incident response plan to include procedures for carrying out digital forensics.
10. Increase communication between the OS SOC and ESOC by allowing reciprocal access to ticketing systems or creating a common system.
11. Establish a timeline to ensure that the systems responsible for endpoint protection are properly authorized.
12. Establish a procedure to ensure sufficient government oversight is provided to contractors who are responsible for OS endpoint protection.
13. Establish tracking and reporting processes to ensure OS OCIO cybersecurity policies and procedures are developed, up to date, and in compliance with federal requirements.
14. Identify which improvement opportunities within the OS OCIO remediation plan should be prioritized to enhance OS' incident detection and response.