Report in Brief

February 11, 2020

Background

Enterprise Web Solutions (EWS) is a document management system used by the Department of Commerce's (the Department's) Office of the Secretary (OS), and is located in Department headquarters in Washington, DC. EWS is provided by a U.S.-based contractor that had a subcontract with a Canada-based company. The Canadian subcontractor was specifically selected to support the EWS system because it was the developer of the document management software. Accordingly, the Canadian subcontractor maintained EWS software and provided user training. The Office of the Chief Information Officer (OCIO) manages the servers hosting EWS, which includes patching the operating system and backing up the system's data. OCIO is also responsible for the overall security of EWS with the exception of vetting contract staff, which is overseen by Department contracting officers.

Why We Did This Review

Our audit objectives were to determine whether the (1) processes used to vet contract staff given administrative access to the EWS system are adequate; (2) Department followed a sufficient process to identify the impact level of the EWS system; (3) OCIO took appropriate actions to protect the information on the EWS system after it was granted an authorization to operate in 2018; and (4) contract used to procure EWS services and systems complied with Department acquisition regulations. Because of the serious nature of the cybersecurity issues identified, we determined that this audit report would address the first three objectives, while a separate, follow-on audit may address the fourth.

OFFICE OF THE SECRETARY

Failures in the Department's Security Program Resulted in Exposure of Sensitive Trade Information to Unvetted Foreign Nationals

OIG-20-018-A

WHAT WE FOUND

We found that (1) the Department exposed sensitive data to unvetted foreign nationals working outside the United States; (2) unauthorized foreign nationals accessed and modified the EWS system after their contract had been terminated; (3) the Department mishandled the response to unauthorized access by foreign nationals; and (4) the Department failed to account for sensitive data on its systems.

WHAT WE RECOMMEND

We recommend that the Deputy Secretary of Commerce ensure that OCIO does the following:

1. Implements additional checks into contract policies and procedures to ensure all access to Department systems and data is properly vetted by the Department's Office of Security (OSY).
2. Conducts a thorough review of the contractor and subcontractor access granted to all Department systems and ensures this access is limited and appropriate based upon the purpose of the system, data contained on the system, and the contractor's level of required duties.
3. Establishes and implements a process that ensures the information system security officer(s) or other assigned system staff regularly validate that user access to Department systems is appropriate.
4. Fully documents its rationale, based upon the outcome of the Department's investigation, for not reporting the exposure of sensitive data from the former Secretary's briefing book as a major incident, as defined by Office of Management and Budget guidance.

We recommend that the Deputy Secretary of Commerce ensure that OSY does the following:

5. Investigate the Department's mishandling of sensitive briefing book data in accordance with its security policies.

We recommend that the Deputy Secretary of Commerce ensure that OCIO does the following:

6. Establishes and follows clear procedures when revoking access to Department systems, a process that should include the system owner, information system security officer, and contracting officer's representative, when appropriate.
7. Reviews and revises incident response procedures so that appropriate communication protocols are established and enforced to ensure timely and accurate information sharing.
8. Identifies staff with incident response and system recovery roles and ensure that they have regular training regarding their responsibilities, the role of the Enterprise Security Operations Center, and the use of system backups.
9. Includes an additional step to review the completed task when revoking system access, with a requirement for assignment of an individual responsible for ensuring all access has been removed.
10. Reviews and revises the process used for system impact analysis to ensure that it is sufficiently rigorous and has adequate checks to ensure the process produces accurate results.
11. Reassess all OS systems to ensure that the designated impact level analyses are accurate and appropriate to protect Department systems.
12. Determines if any systems outside of OS produce data for the Secretary's briefing book and, if systems are identified, determines if these systems have accurate and appropriate system impact levels.