Report in Brief

June 15, 2022

Background

The U.S. Department of Commerce (the Department) operates national security systems (NSS) within several of its offices and bureaus. NSS are information technology (IT) systems that store, process, or communicate classified information and, by their very nature, represent some of the greatest IT security risks within the Department. Prior to a reorganization in December 2016, the National Security Programs and Operations office within the Department's Office of the Chief Information Officer (OCIO) was responsible for the Department's national security IT program. Following this reorganization, the Department created the National Security Solutions and Services (NS3) team within OCIO, which became responsible for both overseeing the implementation of the Department's national security IT program as well as managing several NSS. In 2019, NS3 underwent a leadership change, and at the end of our fieldwork in January 2022, the NS3 director left his position. In March 2022, the Department Chief Information Officer became the acting NS3 director.

Why We Did This Review

The objective of our evaluation was to determine whether the Department and its bureaus are managing NSS in compliance with federal and Departmental IT security requirements.

OFFICE OF THE SECRETARY

The Department Mismanaged, Neglected, and Wasted Money on the Implementation of IT Security Requirements for Its National Security Systems

OIG-22-023-I

WHAT WE FOUND

We found that the Department mismanaged and neglected IT security requirements for its NSS. We also found that the Department wasted at least $380,000 on an NSS that it did not use. These issues indicate that the Department's national security program has significant deficiencies, which placed these systems at risk and deprived resources from being effectively used. Until the Department takes actions to strengthen efforts to immediately address these deficiencies, longstanding and pervasive issues will likely continue to jeopardize the IT security posture of its NSS.

WHAT WE RECOMMEND

We recommend that the Deputy Secretary of Commerce ensure that the Chief Information Officer does the following:

1. Implement the following Committee on National Security Systems and National Institute of Standards and Technology IT security requirements for System X: (a) fill fundamental security roles (e.g., system owner, information system security officer); (b) complete the risk management framework steps, including authorizing System X to operate; (c) develop a process to regularly install software security updates; and (d) replace end-of-life system components.
2. Implement multi-factor authentication for access to all of the Department's NSS according to Committee on National Security Systems requirements.
3. Define and convey which responsibilities OCIO will provide regarding a multi-factor authentication infrastructure.
4. Perform an organizational review to ensure all of the Department's NSS receive sufficient oversight and resources to conduct required security activities.
5. Immediately develop detailed policies and procedures that will do the following: (a) ensure the authorization process for Departmental NSS is clearly defined and executed according to the risk management framework; (b) require that Department NSS receive regular, independent assessments according to the risk management framework. These policies and procedures must include consideration of security clearance adjudication timeframes for future assessments; and (c) address the creation and maintenance of an NSS inventory. This should include a requirement for all Department bureaus to provide an update when changes occur.