Report in Brief

December 17, 2024

Background

The Enterprise Continuous Diagnostics and Mitigation (ECDM) program is a critical part of the U.S. Department of Commerce's (the Department's) strategy for meeting its cybersecurity modernization goals and transitioning to a Zero Trust Architecture by the end of fiscal year 2024. ECDM is the Department's implementation of the Continuous Diagnostics and Mitigation (CDM) program in collaboration with the U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA). The Department deploys security tools procured via CISA's CDM program across all Department bureaus to provide enterprise-wide visibility into security for reporting, risk management, continuous monitoring, and incident response. CISA uses the Department's cybersecurity data collected via ECDM to assess, track, and respond to cybersecurity threats across all federal agencies. The Department operates the ECDM program through a National Institute of Standards and Technology (NIST)-managed information system.

Our previous audit work found the Department faces challenges in meeting ECDM program goals. The Department and CISA told us the biggest risk the ECDM program currently faces is a deficiency in asset visibility. Effective cybersecurity efforts hinge on accurate asset discovery and management—the Department cannot secure unseen and untracked assets, and subsequent cybersecurity capabilities, such as vulnerability management and incident response, are built on this cornerstone.

Why We Did This Review

Our audit objective was to assess the effectiveness of the Department's ECDM program.

OFFICE OF THE SECRETARY

Data Quality Challenges and Ineffective Program Management Hinder the Department's Enterprise Cybersecurity Capabilities

OIG-25-006-A

WHAT WE FOUND

We found that the Department has not yet adequately strengthened its cybersecurity posture by fully implementing its ECDM program. Specifically, we found the following:

I. ECDM data quality does not fully support Department oversight and reporting needs.

II. NIST does not consistently control and thoroughly test the ECDM program's information system changes.

III. The ECDM program's information system is relatively secure but has some internal security weaknesses.

IV. Deficiencies in ECDM program management place future enterprise cybersecurity tool deployments at risk.

V. The Department does not fully incorporate bureau-incurred costs in its ECDM project cost tracking.

Remediating these deficiencies is important to ensure the ECDM program achieves the goals of reducing the Department's threat surface, increasing cybersecurity visibility, improving response capabilities, and streamlining reporting.

WHAT WE RECOMMENDED

We recommended that the Deputy Secretary of Commerce direct the Department's Chief Information Officer to:

- Develop and implement oversight mechanisms to manage and track whether bureaus meet hardware asset management, software asset management, configuration security management, and vulnerability management data collection and reporting requirements. Implementing this recommendation will lead to funds being put to better use.
- Develop and implement oversight mechanisms to ensure Department cybersecurity data reported in the CDM agency dashboard and used in Chief Information Officer Federal Information Security Modernization Act metric reporting accurately reflects the Department's cybersecurity posture.
- Incorporate the Office of Acquisition Management's project management best practices into the ECDM program and ensure program and project managers overseeing the ECDM program obtain a level I Federal Acquisition Certification for Program and Project Managers.
- Design and implement a process to track and report bureau-incurred ECDM program costs for improved cost reporting and analysis of cost-saving opportunities.

We recommended that the Deputy Secretary of Commerce direct the Department's Chief Information Officer and NIST's Chief Information Officer to:

- Design and implement a technical control to prevent changes to the production environment without proper configuration change control processes and testing.
- Implement logging for the security policy changes identified by our testing.
- Review our detailed technical report and develop and implement a corrective action plan to resolve the issues we identified in our penetration testing.