Report in Brief

January 25, 2022

Background

Managing organizational risk is paramount to an effective information technology (IT) security program. Federal information systems undergo continuous change from expanding user bases, hardware and software upgrades and additions, and new internal and external threats. The U.S. Department of Commerce (the Department) depends on its information systems to continue to protect the confidentiality, integrity, and availability of the data and services they host. Unfortunately, the Department's IT security program continually underperforms, largely due to the inconsistent implementation of its defined IT security policies and procedures.

We previously noted that the overall maturity of the Department's IT security program had not progressed since 2017. We conducted this audit in response to repeated issues surrounding the Department's overarching implementation and maturity of its IT security program. Our audit work focused on identifying potential shortfalls in the Department's implementation of the *Assess* and *Monitor* steps in the Risk Management Framework developed by the National Institute of Standards and Technology as required by federal law.

Why We Did This Review

Our audit objective was to assess the effectiveness of the Department's system security assessment and continuous monitoring program to ensure security deficiencies were identified, monitored, and adequately resolved.

OFFICE OF THE SECRETARY

The Department Needs to Improve Its System Security Assessment and Continuous Monitoring Program to Ensure Security Controls Are Consistently Implemented and Effective

OIG-22-017-A

WHAT WE FOUND

We found that the Department did not effectively execute its continuous monitoring and system assessment process. Specifically, we found the following:

I. The Department did not effectively plan for system assessments.

II. The Department did not consistently conduct reliable system assessments.

III. The Department did not resolve security control deficiencies within defined completion dates.

IV. The Department's security system of record—i.e., the cyber security asset and management (CSAM) tool—did not provide accurate and complete assessment and plan of action & milestone (POA&M) data.

WHAT WE RECOMMEND

We recommend that the Department's Chief Information Officer ensure that bureau Chief Information Officers do the following:

1. Implement tracking and reporting verifying that (1) assessment planning procedures are documented prior to the execution of an assessment and (2) system security documentation is accurate.
2. Hold IT security staff accountable for the quality and effective execution of preassessment and assessment processes.
3. Verify that assessment supporting documentation is maintained and sufficiently supports assessment results to facilitate oversight.
4. Determine why POA&M dates are not achievable.
5. Using the analysis from Recommendation 4, provide guidance for how to better plan, prioritize, and resolve POA&Ms within their established milestones.
6. Hold individuals accountable for not resolving issues within established milestones.

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

7. Work with Department bureaus to automate and customize CSAM data entry to ensure CSAM accurately reflects bureau data.
8. Provide additional CSAM usability training.