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

FINAL REPORT NO. OIG-22-017-A
JANUARY 25, 2022

U.S. Department of Commerce
Office of Inspector General
Office of Audit and Evaluation

UNITED STATES DEPARTMENT OF COMMERCE
Office of Inspector General
Washington, D.C. 20230

January 25, 2022

MEMORANDUM FOR: André Mendes
Chief Information Officer

FROM: Frederick J. Meny, Jr.
Assistant Inspector General for Audit and Evaluation

SUBJECT: *The Department Needs to Improve Its System Security Assessment and Continuous Monitoring Program to Ensure Security Controls Are Consistently Implemented and Effective*
Final Report No. OIG-22-017-A

Attached for your review is the final report on the audit of the U.S. Department of Commerce's (the Department's) system security assessment process. The objective of this audit 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.

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 tool—did not provide accurate and complete assessment and plan of action & milestone data.

On December 22, 2021, we received the Department's response to our draft report. We also received technical comments. Based on those technical comments, we made changes to the final report where appropriate. In response to the draft report, the Department concurred with all of the recommendations and described actions it has taken, or will take, to address them. The Department's formal response is included within the final report as appendix D.

Pursuant to Department Administrative Order 213-5, please submit to us an action plan that addresses the recommendations in this report within 60 calendar days. This final report will be posted on OIG's website pursuant to sections 4 and 8M of the Inspector General Act of 1978, as amended (5 U.S.C. App., §§ 4 & 8M).

We appreciate the cooperation and courtesies extended to us by your staff during our audit. If you have any questions or concerns about this report, please contact me at (202) 482-1931 or Chuck Mitchell, Director for Cybersecurity, at (202) 809-9528.

Attachment

cc: MaryAnn Mausser, Audit Liaison, Office of the Secretary
Joselyn Bingham, Audit Liaison, OCIO
Ryan Higgins, Chief Information Security Officer, OCIO
Phillip G. Lamb, Director, Security Program Management Services, OCIO
Maria Hishikawa, IT Audit Liaison, OCIO

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.

Contents

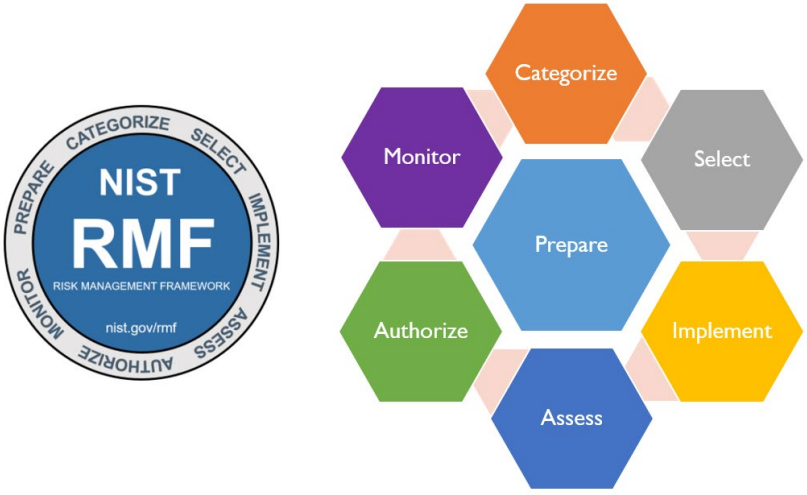
Cover: Herbert C. Hoover Building main entrance at 14th Street Northwest in Washington, DC. Completed in 1932, the building is named after the former Secretary of Commerce and 31st President of the United States.

Introduction

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.

In our fiscal year (FY) 2021 *Top Management and Performance Challenges Facing the Department of Commerce* report,[1] we noted the overall maturity of the Department's IT security program had not progressed since 2017—the effects of which were seen throughout several recent audit reports. 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 (RMF)[2] developed by the National Institute of Standards and Technology (NIST) as required by federal law.[3] Figure 1 illustrates this framework.

Figure 1. NIST RMF



Source: https://csrc.nist.gov/projects/risk-management/about-rmf

[1] U.S. Department of Commerce Office of Inspector General, October 15, 2020. *Top Management and Performance Challenges Facing the Department of Commerce in FY 2021*, OIG-21-003. Washington, DC: DOC OIG, pgs. 24–25.

[2] DOC National Institute of Standards and Technology, December 2018. *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, NIST Special Publication 800-37, Revision 2. Gaithersburg, MD: NIST. Available online at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf (accessed August 12, 2021).

[3] Federal Information Security Modernization Act of 2014, 44 U.S.C. § 3551 *et seq.*

The RMF process integrates security and privacy management activities into the system development life cycle and provides detailed guidance in the form of NIST Special Publication (SP) documents—predominantly the SP 800 series focusing on information security[4] (e.g., NIST SP 800-53). There are seven steps in the RMF process; each step builds off the previous one. Appendix B provides a more detailed description of each RMF step. Proper implementation of the RMF—specifically in assessment and monitoring—can provide the means to achieve effective management of information security risk through a repeatable process by ensuring implementation of security controls.

[4] DOC NIST Computer Security Resource Center. *NIST Special Publication 800 Series documentation* [online]. https://csrc.nist.gov/publications/sp800 (accessed July 12, 2021).

Objective, Findings, and Recommendations

The objective of this audit 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. Appendix A provides a more detailed description of our audit objective, scope, and methodology.

We found 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.

Without an effective process to plan, execute, and monitor system assessments, systems may be compromised due to ineffective security controls. The Department has been responsive to our previous audit findings and subsequently implemented initiatives to address its shortcomings related to continuous monitoring. According to the Department's Office of the Chief Information Officer, the initiatives include (1) updating the enterprise-wide risk management tool, (2) establishing working groups to track and monitor assessment processes across Departmental bureaus, and (3) developing training material to better guide bureaus in implementing required policies and procedures. However, the Department had not fully implemented these updates at the time of this audit, and we continued to find persistent deficiencies in the implementation of information security policies and processes.

I. The Department Did Not Effectively Plan for System Assessments

Security control assessments are a pivotal step in maintaining the Department's IT security program. These assessments identify shortcomings in an organization's implementation of the RMF process. Due to the importance and complexity of a security control assessment, preparation is essential. Planning establishes standards and expectations between involved parties prior to an assessment. Additionally, system assessors are independent of the system they assess; therefore, they rely on planning and current system security documentation to guide their efforts. We analyzed FY 2020 preassessment documentation across our sample of 54 systems[5] and determined the Department did not effectively plan for assessments.

[5] See appendix A, bullet 2, for more detail on our statistical sampling methodology.

A. Assessment planning was inconsistent and did not provide a reliable foundation to conduct assessments

To guide planning at an enterprise level, the Department requires that all bureaus develop security assessment plans (SAPs) to include, at a minimum, three main components: (1) all security controls and control enhancements under assessment; (2) the assessment procedures to be used; and (3) the assessment environment, the people involved, and their roles and responsibilities.[6] A well-defined SAP provides other essential information, including the system's unique assessment needs, timelines, control assessment requirements, and accountability through assigning assessor roles and responsibilities.

To determine how well the Department planned assessments, we reviewed documentation provided by the Department's bureaus and found that an estimated 122 of the 256 systems (48 percent) produced consolidated SAPs prior to assessments. For the remaining 134 systems (52 percent) without SAPs, bureaus depended on alternative planning measures; however, they did not consistently implement those measures across all organizational systems. In our effort to determine whether the provided SAPs or bureau alternative planning measures met Department policy, we compared all planning documents against the minimum SAP requirements previously listed. After taking into consideration nonstandardized processes, we found planning efforts for an estimated 118 systems (46 percent) still did not meet Department-prescribed requirements. More notably, adequate testing methods[7]—which provide assessors with tailored guidance on how to assess a system—were not established during planning for an estimated 138 FY 2020 assessments (54 percent). As a result, we found that assessors relied on ad hoc or untailored NIST guidance, which does not take into account each individual system's specific needs. This lack of preparation in conjunction with an assessor's limited system background knowledge could result in unassessed system components or control elements.

We contacted noncompliant bureaus to determine why required planning steps were not included as a part of their assessment process. One bureau reported that it preferred to plan as it goes, rather than at the beginning of the assessment. One bureau relied only on general NIST SP 800-53A[8] guidance, and four others stated that noncompliance was due to delayed implementation or lack of due diligence by staff. The inconsistency in assessment planning across the Department suggests a poor foundation for the assessment process—which, as seen in forthcoming findings, permeates

[6] DOC, June 2019. *Department of Commerce Information Technology Security Baseline Policy (ITSBP)*, Version 1.0. Washington, DC: DOC, Annex B-4: Security Assessment and Authorization (CA) ITSBP Requirements.

[7] DOC NIST, April 2013. *Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans*, NIST Special Publication 800-53A, Revision 4. Gaithersburg, MD: NIST, 10. Available online at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf (accessed August 13, 2021). NIST describes an assessment method as examining, interviewing, or testing to obtain evidence during an assessment.

[8] *Ibid*.

throughout the entire process. Without adequate planning, the Department cannot effectively implement the assessment step of the RMF.

B. *System security plans (SSPs) do not accurately relay critical security information*

SSPs hold the bulk of system security information, making them the fundamental security document of federal information systems. While there are many sections to an SSP, we focused on security control implementation details[9] assessors rely on to conduct assessments (see appendix C, figure C-1).

Although Department policy[10] requires that bureaus annually review and update SSPs to reflect system changes, we found that SSPs were not always accurate. The Department tailors the implementation of several security controls and requires its bureaus to implement those tailored changes. Tailored changes include additional control requirements that supplement standard NIST SP 800 guidance, such as requiring staff to upload system security documentation (e.g., configuration management plans, contingency plans, and incident response plans) into the Department's enterprise-wide CSAM tool, which maintains inventory, security, and risk data for all Departmental systems. Of the systems we tested, we found that only the U.S. Census Bureau (the Census Bureau) included these requirements in its SSPs. Consequently, our analysis found that the Department's additional requirements were absent from an estimated 212 of the SSPs (83 percent) for the 256 systems. Further, of the systems we tested, 1 SSP for the National Telecommunications and Information Administration did not have security control requirements, and 9 Census Bureau SSPs were missing one or more required implementation statements.[11] Assessors cannot provide assurance of security control implementation if the requirements themselves are inaccurate or missing, ultimately jeopardizing a system's security.

We also found incorrect control status (satisfied or not satisfied) and control inheritance[12] information. Mislabeling these important fields in an SSP can result in the assessor not reviewing the control with the appropriate methodology. For example, assessors have reported that they do not always reassess inherited controls since the providing system assesses the control; instead, they review the control's status and

---

[9] DOC NIST, February 2006. *Guide for Developing Security Plans for Federal Information Systems*, NIST Special Publication 800-18, Revision 1. Gaithersburg, MD: NIST, pgs. 24–25. Available online at https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-18r1.pdf (accessed August 13, 2021). According to NIST, "[t]he [control] description should contain 1) the security control title; 2) how the security control is being implemented or planned to be implemented; 3) any scoping guidance that has been applied and what type of consideration; and 4) indicate if the security control is a common control and who is responsible for its implementation."

[10] DOC *ITSBP*, Annex B-12: Planning (PL) ITSBP Requirements.

[11] Security control requirements describe what capabilities should be implemented on a system. Implementation statements describe how those capabilities are actually put in place.

[12] Control inheritance describes instances where another party is responsible for control; that party can be internal or external to the organization. See appendix C, figure C-1, for additional details.

confirm. While this is not out of normal procedure, it could cause an issue if controls are mislabeled.

SSPs relay critical security information to assessors and other personnel who depend on the information to make informed security-related decisions. For this reason, accuracy and completeness of implementation details are vital. Multiple bureaus reported that SSP maintenance suffered due to lack of due diligence by staff, while some asserted that they would update plans in conjunction with the implementation of new NIST guidance. However, the Department's tailored requirements had been in place since 2019, giving bureaus ample time to incorporate them into their SSPs. The amount of inaccuracies in the bureaus' SSPs indicates a pervasive problem with the Department's ability to manage its system security documentation and shows that system staff lack familiarity with their systems and Department policy.

Recommendation

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.

II. The Department Did Not Consistently Conduct Reliable System Assessments

Once planning activities are concluded, the assessment team begins the assessment process. This determines whether security controls are functioning as intended and protecting organizational data. Department policy[13] establishes (1) a set of minimum requirements around the system assessments, including how often they should take place, and (2) a set of 15 continuous monitoring controls[14] bureaus must annually assess. In addition, Department policy dictates that bureaus must conduct or enter assessments in CSAM[15] and carry out their work in accordance with NIST SP 800-53A standards.[16] Beyond that, the Department grants bureaus significant flexibility in establishing their own processes. We analyzed assessment documentation across our sample of 54 systems[17] and determined the Department was not effectively executing its system assessments.

[13] DOC *ITSBP* requires that bureaus assess a subset of system controls on an annual basis.

[14] The Department prescribes that bureaus either (1) assess a subset of controls annually, to include 15 continuous monitoring controls, or (2) develop their own risk-based methodology and continuous monitoring requirements. With the exception of the Census Bureau, all other bureaus implement option 1. See appendix C, table C-1, for the 15 continuous monitoring controls.

[15] DOC *ITSBP*, Annex B-4: Security Assessment and Authorization (CA) ITSBP Requirements.

[16] "[Bureaus] must use NIST Special Publication 800-53A, Revision 4, as amended, as the basis for assessing information system security controls to determine the extent to which they are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements." DOC *ITSBP*, p. 11.

[17] See appendix A, bullet 2, for more detail on our statistical sampling methodology.

A. *The Department did not consistently assess core minimum security controls for its high- and moderate-category systems*

We reviewed system assessment results against the core minimum Department requirements. Our analysis found that the Department did not consistently assess core minimum controls for an estimated 114 of 256 systems (44 percent) over the past 3 years. These controls are the Department's annual minimum requirements, indicating that they are so important they should be reviewed every year. They include controls that provide security capabilities that protect system data, such as account management, audit review, analysis, and vulnerability scanning (see appendix C, table C-1).

More concerning, we found that an estimated 51 of the 256 systems (20 percent) that we tested operated for a year or more without having any level of independent assessment. We found examples in the National Oceanic and Atmospheric Administration, the Bureau of Industry and Security, the United States Patent and Trademark Office, the International Trade Administration, and the Office of the Secretary. Two of the systems were high value assets (HVAs)[18] considered critical to the Department's ability to carry out its mission.[19] Additionally, for 3 years, the International Trade Administration did not assess its common controls package,[20] which multiple systems depended on for security control capabilities. During these periods, management had no assurance that unassessed controls were protecting critical organizational data. Management reported various reasons for noncompliance including insufficient resources, contract conflicts, and poor oversight.

Assessments not only identify system vulnerabilities, they also initiate the process that ensures vulnerability remediation. Therefore, it is imperative that assessments are conducted within defined timeframes to ensure controls are continuously functioning as intended.

B. *Documentation supporting system assessment results was not always available for review, limiting the Department's potential for oversight and quality control*

To determine the quality of assessments, we compared each system's FY 2020 assessment evidence for the 15 continuous monitoring controls[21] against NIST-prescribed formats[22] (see appendix C, figure C-2), which break control requirements down to a granular level to ensure all elements are addressed. However, evidence did

[18] HVAs are "[t]hose information resources, mission/business processes, and/or critical programs that are of particular interest to potential or actual adversaries." *See* DOC NIST CSRC. *High Value Asset (definition)* [online]. https://csrc.nist.gov/glossary/term/high_value_asset (accessed June 24, 2021).

[19] Both HVAs were assessed in FY 2021.

[20] A *common control* is "[a] security control that is inherited by one or more organizational information systems." *See* DOC NIST CSRC. *Common control (definition)* [online]. https://csrc.nist.gov/glossary/term/common_control (accessed June 24, 2021).

[21] See appendix C, table C-1, for the list of controls.

[22] NIST prescribes that assessments be performed using "determine if" statements, as they "provid[e] the capability to identify and assess specific parts of security and privacy controls." *See* DOC NIST, *Assessing Security and Privacy Controls*, p. vi.

not always provide enough detail to perform comprehensive oversight using this method. With the exception of the Census Bureau, assessment data only provided high-level summaries that were not broken down by control requirement. Evidence varied greatly across bureaus, ranging from well-detailed data to none at all. In fact, evidence for an estimated 56 of 256 systems (22 percent) was so vague that we could not conclude with certainty what artifacts, if any, were assessed. CSAM's required assessment tool includes necessary attributes that would allow for proper oversight and validation of the assessment process; however, an estimated 237 systems (93 percent) did not use the tool. Without sufficient documentation, management cannot perform proper quality control and ensure assessments meet standards and organizational expectations.

Through the RMF, NIST has prescribed a process for periodic assessment of security controls protecting systems. Based on our analysis, the Department cannot depend on its implementation of RMF to ensure controls are functioning as intended and safeguarding organizational data.

Recommendations

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

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.

III. The Department Did Not Resolve Security Control Deficiencies Within Defined Completion Dates

After an assessment identifies a security weakness or deficiency, a POA&M must be developed to address the vulnerability. Every individual POA&M provides the Department insight into what security weaknesses the Department faces and how effectively the Department corrects those weaknesses. We reviewed POA&M documentation across our sample of 54 systems[23] and determined the Department was not effectively managing POA&Ms.

Department policy[24] requires the Authorizing Official (AO) to establish realistic, achievable timelines for POA&M completion based on prioritization and resource availability. Personnel must also update POA&Ms every month[25] to keep POA&M progress current. The Department requires[26] that bureaus track and manage POA&Ms in the centralized

[23] See appendix A, bullet 2, for more detail on our statistical sampling methodology.

[24] DOC *ITSBP*, Annex C-13: Plans of Action and Milestones (POA&M), 6.2.7. *Assign Scheduled Completion Date*.

[25] DOC *ITSBP*, Annex C-13: Plans of Action and Milestones (POA&M), 6.2.9. *Monitor and Report POA&M Activity*.

[26] DOC *ITSBP*, Annex B-4: Security Assessment and Authorization (CA) ITSBP Requirements.

CSAM tool. Security personnel establish two separate date fields for the overall POA&M completion date. The "scheduled completion date" is used by the Department to determine a POA&M's delay status. The second date, called the "planned finish date," provides security personnel a method to alter the POA&M completion date during monthly status updates in case there are delays.

We reviewed the Department's monthly POA&M status report and noted that 584 active POA&Ms have missed their scheduled completion date milestones by at least 180 days as of March 2021.[27] The Census Bureau and the United States Patent and Trademark Office represent more than 500 of the overdue POA&Ms. The report includes POA&Ms for operational systems reportable under the Federal Information Security Modernization Act of 2014 (FISMA) in CSAM and provides insight into (1) the effectiveness of setting a milestone and (2) the length of time an unresolved security control failure affects the system past the scheduled completion date. This is important because AOs approve a system's use based on known risks. When POA&Ms go beyond their scheduled completion date, the risk may be above what is acceptable to operate those systems.

To understand how well system security staff actively managed POA&Ms, we compared 5 years of each system's POA&M planned finish dates against the actual finish dates.[28] We determined that an estimated 132 of 256 systems (52 percent) had POA&Ms that missed their planned finish date milestones by 30 days or more. We found examples from a majority of the bureaus in our sample. Since the planned finish date is modifiable, this indicates that staff did not actively manage POA&M dates to provide a more realistic timeline.

CSAM provides a standardized set of reasons for delays. Some reasons reported include technical implementation delays, personnel shortages, contractual issues, insufficient funding, priority changes, policy delays, and underestimating the original completion date, among other things. During our follow-up with system security staff, they indicated operational overhead issues when updating POA&Ms. One bureau reported that CSAM does not currently allow bureau personnel to update POA&Ms in bulk. Bureau staff also attributed inadequate POA&M management to a lack of training and guidance with regard to POA&M development and updating. Although security staff cited various reasons for the delays, we were unable to determine a common root cause.

Allowing security weaknesses and deficiencies to go unresolved 6 months or more from the approved resolution date leaves systems operating with a level of risk that the AO may not have anticipated during the system's authorization. In the case of POA&Ms, that risk means

[27] The Department's monthly POA&M report aggregates data from all of its bureaus. The Department's status report relies on the "scheduled completion date" to calculate number of days delayed. As of September 2021, the Department has reported 403 active POA&Ms that are overdue by at least 180 days. This new information was subsequent to our testing and not validated by us.

[28] In instances where the POA&M was in progress and an actual finish date was not available, we reviewed to see if the POA&M was still open beyond the planned finish date.

unresolved security control failures that may provide a weakness for exploitation by attackers, leading to system compromise.

Recommendations

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

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.

IV. The Department's Security System of Record—i.e., the CSAM Tool—Did Not Provide Accurate and Complete Assessment and POA&M Data

The Department relies on CSAM to provide visibility of IT risk across all bureaus. CSAM's primary function is to facilitate the RMF process at an enterprise level. Department policy[29] requires that bureaus input system inventory attributes, assessment information, and POA&Ms into CSAM. The Department then utilizes CSAM data to track IT security risk and maintain inventory. To determine if the Department's data was reliable, we reviewed CSAM inventory data for all operational systems and attempted to reconcile data in CSAM against self-reported data in the 54 systems[30] we sampled.

In reviewing CSAM inventory data,[31] we found inaccurate and missing attributes that identify and categorize the Department's systems. Over half of the systems were missing data fields such as Business Identifiable Information, Cloud System Status, and HVA status. More concerning, two of the systems with blank HVA status were tracked as HVAs by other Department sources. As stated in finding II, HVA status is particularly important because these systems are mission critical and carry additional security and compliance requirements.

We then reviewed to determine if CSAM included FY 2020 system assessment and POA&M data for our sample systems. We were not able to obtain complete assessment data[32] for an estimated 185 of 256 systems (72 percent). CSAM did contain some information, like assessment reports; however, these reports alone do not provide enough data to validate the quality of assessment and track compliance with policies. If assessment data is incomplete in CSAM, the Department has to manually collect it through data calls, creating

[29] DOC *ITSBP*, Annex B-18: Program Management (PM) and Annex B-4: Security Assessment and Authorization (CA).

[30] See appendix A, bullet 2, for more detail on our statistical sampling methodology.

[31] Analysis for this section used a total population of 545 of the Department's low-, moderate-, and high-impact systems with an 'Operational' status in CSAM.

[32] Complete assessment data is defined as an assessment report that includes evidentiary support.

unnecessary work. Additionally, as noted in finding II, most bureaus do not retain the same quality of data that CSAM's automated templates would produce.

We also found that bureaus did not always report identified risk in CSAM. Of the systems that we tested, we found that systems from bureaus responsible for overseeing the nation's weather services, ensuring effective export control, and providing economic data about U.S. citizens did not always enter POA&Ms into CSAM. Although they did internally track mitigation efforts, the Department has limited visibility over internal bureau data. Overall, all identified weaknesses for an estimated 129 systems (50 percent) were not tracked as POA&Ms in CSAM. Leadership depends on this data to produce analytical deliverables for stakeholders. Based on our analysis, the Department is utilizing incomplete information to make risk-based decisions and allocate resources.

Bureaus reported that they internally track system risk data; thus, CSAM requirements create duplicate work. Yet only two bureaus from our sample (the Census Bureau and NIST) reported that they rely on tools other than CSAM as a risk management solution. Staff also reported that technological limitations (e.g., lack of customization and automation) and lack of training have made them reluctant to use the tool. CSAM is the Department's primary centralized risk management solution. Because the Department has not successfully maintained CSAM, it is not sufficiently reliable as an oversight tool. This lack of a reliable tool that centralizes security data limits the Department's ability to effectively oversee information security and assess risk.

Recommendations

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.

Summary of Agency Response and OIG Comments

In response to our draft report, the Department concurred with all of our recommendations and described actions it has taken, or will take, to address them. The Department also provided technical comments recommending changes to the factual and technical information in the report. We accepted the technical comments, as appropriate, and included them in the final version of this report. The Department's formal response is included within this final report as appendix D.

We are pleased that the Department concurs with our recommendations and look forward to reviewing its proposed audit action plan.

Appendix A: Objective, Scope, and Methodology

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. To do so, we

- Assessed the reliability of CSAM's data by (1) performing electronic testing, (2) reviewing existing information about the data and the system that produced them, and (3) interviewing agency officials knowledgeable about the data. We determined that the data were sufficiently reliable for the purposes of this report.
- Analyzed a sample of 54 IT systems throughout the bureaus, in which observations were projected across the Department. Our sample of 54 systems was derived from a universe of 256 of the Department's systems with the following attributes: high- and moderate-impact, operational status, and reportable under FISMA. Resources would not allow the review of the entire population of 256 systems within a time period that produces timely and relevant results. Statistical sampling will allow inference to the population within a satisfactory confidence interval of 90 percent and a margin of error of no more than 10 percent.
- Reviewed the following guidance and regulations:
    - NIST SP 800-53A, Revision 4;
    - DOC *ITSBP*, Version 1;
    - Bureau IT security manuals; and
    - System-related artifacts, assessor workbooks, and any other necessary documentation.
- Interviewed staff from the Department's Office of the Chief Information Officer responsible for (1) developing IT policies, procedures, and operational guidelines and (2) monitoring the Department's overall security posture.

We employed a comprehensive methodology to review internal and external IT security requirements within the context of our audit objective to determine the effectiveness of the Department's continuous monitoring and system assessment process. We broke our work down into the following subobjectives:

- **Subobjective A**—To determine whether the Department adequately identified deficiencies, we requested preassessment and assessment supporting data from all sampled systems and executed a series of test steps. In instances where we were not able to collect data for requested years, we tested the system's most current data, if available.

  - To determine adequacy of planning, we reviewed FY 2020 SAPs for the presence of all Department-required SAP components.[33] In instances where SAPs were unavailable, we tested alternative planning documentation. Next, to determine if system SSPs were reliable sources for security control status information, we reviewed FY 2020 SSPs to validate the accuracy of implementation details.[34]
  - To determine the adequacy of assessment execution, we reviewed assessment results for FYs 2018 through 2020 to validate that each year included the Department's required 15 continuous monitoring controls.[35] We then compared each system's FY 2020 assessment supporting evidence against NIST standards[36] to determine the quality of assessment procedures performed.
  - To determine if assessor independence was maintained, we compared system security staff in SSPs against identified assessors in assessment data and SAPS to confirm there was no overlap.

- **Subobjective B**—To determine whether the Department adequately resolved identified deficiencies, we assessed POA&M data contained within CSAM.
  - We exported each sampled system's CSAM POA&M report for a period of 5 years (2016–2020). We then compared each POA&M's modifiable "planned finish date" against its "actual finish date" to validate that POA&Ms met bureau-defined finish dates. We excluded systems that did not have any POA&Ms in CSAM.
  - Next, we reviewed the Department's current CSAM data on all systems reportable under FISMA to determine how often bureaus closed POA&Ms by their scheduled completion date.
- **Subobjective C**—To determine whether the Department adequately monitored system risk, we performed a series of tests on system inventory and risk-related data contained in CSAM.
  - To determine reliability of system inventory data, we examined CSAM inventory for inaccuracies and incompleteness for all Department systems with an 'Operational' status.
  - Next, to determine if sampled systems complied with the Department's requirement to conduct or input assessment data into CSAM,[37] we attempted to reconcile self-reported FY 2020 assessment data with each respective system's assessment data in CSAM. In instances where the data was not recovered using this method, we reviewed CSAM artifacts for the presence of assessment data.

[33] DOC *ITSBP*.

[34] See DOC NIST, *Guide for Developing Security Plans for Federal Information Systems,* pgs. 24–25.

[35] DOC *ITSBP*.

[36] See DOC NIST, *Assessing Security and Privacy Controls*, p. vi.

[37] DOC *ITSBP*, p. C-5-3.

- Lastly, to determine if sampled systems complied with the Department's requirement to track all POA&Ms in CSAM, we compared each system's vulnerabilities reported in FY 2020 security assessment reports against POA&Ms tracked in CSAM. In instances where we could not locate POA&Ms in CSAM, we validated that the bureaus internally managed POA&Ms.

We reviewed bureaus' compliance with the following applicable internal controls, provisions of law, and mandatory guidance:

- The Department's *Information Technology Security Baseline Policy*
- NIST Special Publications:
  - 800-37, Revision 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*
  - 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*
  - 800-53A, Revision 4, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans*

Our review of internal security controls fell into the Control Activities, Information and Communication, and Monitoring components defined in the U.S. Government Accountability Office's *Standards for Internal Control in the Federal Government*.[38] The following security controls, as defined in the *ITSBP* and NIST SP 800-53, were significant to our audit objective:

- CA-2 System Assessment, including control enhancement CA-2(1)—Independent Assessor
- CA-5 Plan of Action and Milestones, including control enhancement CA-5(1)—Automation Support for Accuracy/Currency
- CA-7 Continuous Monitoring
- PL-2 System Security Plans

We identified issues with the implementation of these security controls as described in the Objective, Findings, and Recommendations section of this report.

We conducted our review from November 2020 through June 2021 under the authority of the Inspector General Act of 1978, as amended (5 U.S.C. App.), and Department Organization Order 10-13, as amended October 21, 2020. We performed our fieldwork remotely.

We conducted this performance audit in accordance with generally accepted government auditing standards. These standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

[38] U.S. Government Accountability Office, September 2014. *Standards for Internal Control in the Federal Government*, GAO-14-704G. Washington DC: GAO.

Appendix B: The Risk Management Framework

Appendix B provides a detailed description of the NIST SP 800-37, Revision 2, Risk Management Framework[39] steps:

- **Step 1 (Prepare):** Preparation initiates the RMF process. During this step, management identifies and assigns key roles, establishes a risk strategy, identifies common controls, and performs an organizational risk assessment. Information gathered during this step aids in the execution of the subsequent steps.
- **Step 2 (Categorize):** Security categorization provides a structured way to document the characteristics of an information system. The categorization step also informs organizational risk management processes and tasks by determining the adverse impact of the loss of confidentiality, integrity, and availability of organizational systems and information. The information impact level dictates the system's categorization as a high-, moderate-, or low-impact system.
- **Step 3 (Select):** After an information system has been categorized, the next step is to select and tailor security controls needed to protect the system, then document those in the SSP. The SSP is the fundamental security document of federal information systems and forms the basis of the next steps in the RMF.
- **Step 4 (Implement):** System security staff implement controls from the SSP, then update the SSP with any relevant new information about implementation progress or problems.
- **Step 5 (Assess):** An independent assessment team and Department security personnel build a SAP. The SAP describes in detail what will happen during the assessment and delineates roles and responsibilities. After SAP approval, assessors utilize NIST SP 800-53A[40] guidance coupled with Department-tailored methods to review security controls. After the assessment, the team produces a security assessment report that documents the control deficiencies and delivers recommendations. Department security personnel then create POA&M documents to track and resolve identified security weaknesses and deficiencies. The POA&M details the risk impact level (low to very high), required resources, any milestones, and scheduled completion date.[41]
- **Step 6 (Authorize):** The Department must assign an AO to its federal information systems. The AO is a senior official or executive-level civil servant who is responsible for ensuring the information system is secure. To do so, the AO reviews the security assessment report results, POA&M documentation on identified weaknesses and deficiencies, and other pertinent security information before approving the system for operation.

[39] DOC NIST, *Risk Management Framework*.

[40] DOC NIST, *Assessing Security and Privacy Controls*.

[41] DOC *ITSBP*, Annex C-13: Plans of Action and Milestones (POA&M), 6.2. *POA&M Life Cycle*.

- **Step 7 (Monitor):** The federal information system is continuously monitored for security concerns based on Department and bureau security policies. Security personnel also work to resolve POA&M-documented weaknesses and deficiencies identified during step 5 (i.e., *Assess*).

Appendix C: Facts and Figures

Figure C-1 provides an example of SSP control implementation details.

Figure C-1. Example of Control Implementation Details Found in System Security Plans

CP-10: Information System Recovery and Reconstitution		
Control Description: The organization provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure.		
Control Status		
☐ Implemented	☐ Planned to be Implemented	☐ Not Applicable
Control Inheritance		
☐ Inherited	☐ Hybrid	☐ System-Specific
Common Control Provider (if Inherited or Hybrid): Enter information on who is responsible for control implementation.		
Control Implementation Details		
Enter information on how the security control is being implemented or planned to be implemented, and any scoping or tailoring guidance that has been applied.		

Source: Office of Inspector General (based on NIST's *Guide for Developing Security Plans for Federal Information Systems*, p. 30)

Table C-1 provides the Department's designated 15 continuous monitoring controls.

Table C-1. Department-Defined Continuous Monitoring Controls

Control #	Control Label
AC-2	Account Management
AC-18	Wireless Access Restrictions
AU-3	Content of Audit Records
AU-6	Audit Review, Analysis and Reporting
CM-4	Monitoring Configuration Changes
CM-6	Configuration Settings
CM-7	Least Functionality
CM-8	Information System Component Inventory
CM-9	Configuration Management Plan
CP-2	Contingency Plan

Control #	Control Label
CP-4	Contingency Plan Testing and Exercises
PL-1	Security Planning Policy and Procedures
PL-2	System Security Plan
RA-3	Risk Assessment
RA-5	Vulnerability Scanning

Source: DOC *ITSBP*, p. 201

Figure C-2 provides assessment objectives.

Figure C-2. Assessment Objectives[42]

CP-9	INFORMATION SYSTEM BACKUP		
	ASSESSMENT OBJECTIVE: *Determine if the organization:*		
	CP-9(a)	CP-9(a)[1]	*defines a frequency, consistent with recovery time objectives and recovery point objectives as specified in the information system contingency plan, to conduct backups of user-level information contained in the information system;*
		CP-9(a)[2]	*conducts backups of user-level information contained in the information system with the organization-defined frequency;*
	CP-9(b)	CP-9(b)[1]	*defines a frequency, consistent with recovery time objectives and recovery point objectives as specified in the information system contingency plan, to conduct backups of system-level information contained in the information system;*
		CP-9(b)[2]	*conducts backups of system-level information contained in the information system with the organization-defined frequency;*
	CP-9(c)	CP-9(c)[1]	*defines a frequency, consistent with recovery time objectives and recovery point objectives as specified in the information system contingency plan, to conduct backups of information system documentation including security-related documentation;*
		CP-9(c)[2]	*conducts backups of information system documentation, including security-related documentation, with the organization-defined frequency; and*
	CP-9(d)	*protects the confidentiality, integrity, and availability of backup information at storage locations.*	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS: **Examine**: [*SELECT FROM:* Contingency planning policy; procedures addressing information system backup; contingency plan; backup storage location(s); information system backup logs or records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with information system backup responsibilities; organizational personnel with information security responsibilities]. **Test**: [*SELECT FROM:* Organizational processes for conducting information system backups; automated mechanisms supporting and/or implementing information system backups].		

Source: NIST, *Assessing Security and Privacy Controls*, p. 11

[42] Figure C-2 is an example of a NIST security control assessment procedure. The assessment objectives are broken down by control requirement (e.g., CP-9(a), CP-9(b), and CP-9(c)), which provides a level of granularity necessary to differentiate between requirements.

Appendix D: Agency Response

UNITED STATES DEPARTMENT OF COMMERCE
Chief Information Officer
Washington, D.C. 20230

MEMORANDUM FOR: Peggy E. Gustafson
Inspector General

FROM: André V. Mendes
Chief Information Officer

ANDRE MENDES
Digitally signed by ANDRE MENDES
Date: 2021.12.21 09:53:05 -06'00'

SUBJECT: Department of Commerce Concurrence to the Inspector General's Draft Report, *The Department Needs to Improve Its System Security Assessment and Continuous Monitoring Program to Ensure Security Controls Are Consistently Implemented and Effective (OIG-21-389, November 24, 2021)*

We appreciate that the Office of the Inspector General (OIG) presented the Department of Commerce (DOC) with an opportunity to review the Draft Report, *The Department Needs to Improve Its System Security Assessment and Continuous Monitoring Program to Ensure Security Controls Are Consistently Implemented and Effective (OIG-21-389, November 24, 2021).*

The DOC Office of Chief Information Officer (OCIO) has reviewed the draft report and generally concurs with the finding and recommendations. The DOC OCIO has taken steps to improve our planning process and documentation as discussed with OIG. The DOC is providing the attached comments for OIG's consideration.

Should you have any questions, please contact Ryan A. Higgins at (202) 868-2322 or rhiggins@doc.gov.

Attachments

cc: MaryAnn Mausser
Joselyn Bingham, Audit Liaison
Ryan Higgins, Chief Information Security Officer
Phillip G. Lamb, Director, Security Program Management Services
Maria Hishikawa, IT Audit Liaison

Department of Commerce Technical and Editorial Comments on the OIG Draft Report entitled The Department Needs to Improve Its System Security Assessment and Continuous Monitoring Program to Ensure Security Controls Are Consistently Implemented and Effective (OIG-21-389, November 24, 2021)

The Department of Commerce has reviewed the draft report and we offer the following comments for OIG's consideration. Page numbers refer to page numbers in the draft report unless otherwise stated.

Office of Cybersecurity and IT Risk Management (OCRM)

General Comments

PDF Page 7 (Document Page 3) Objectives, Findings, and Recommendations

"Despite these efforts, we continue to find..." is not in context with the scope of the FY18-21 documents reviewed for this report. The initiatives for updating policies and procedures refer to efforts initiated in FY21 to be fully implemented in FY22, pending document reviews, comments, and approvals. The policy modernization initiative underway, once implemented, will address many of these findings throughout FY22 and beyond. The last sentence may be restated as "Since these efforts are not yet fully implemented, we encourage that our findings be incorporated into these initiatives for addressing and mitigating our findings on persistent deficiencies in the implementation of information security policy and processes."

Recommended Changes for Factual/Technical Information

PDF Page 8 (Document Page 4), Section I: A. Request rewording for clarity: Comments for Finding I: "The Department Did Not Effectively Plan for System Assessments"

The word 'oversight' is used throughout the document with distinctly different meanings, leading to confusion for the reader. The observation is written that oversight by staff members caused the condition to pose risks (also on page 6), while the recommendation is to provide more oversight to complete all tasks without error. When using the word 'oversight' to indicate an error or a misstep, we suggest rewording to "inattention" or "lack of due diligence." The word 'oversight' is used on page 7 and in recommendation #3 to mean 'providing appropriate enforcement and quality assurance for compliance.' We suggest using different words for the condition observed versus the recommendation for clarity when different meanings are being conveyed.

PDF Page 11 (Document Page 7), Section II: A. Request additional context for observation: Comments on Finding II: "The Department Did Not Consistently Conduct Reliable System Assessments"

"Two of the systems were High Value Assets (HVAs) considered critical to the Department's ability to carry out its mission." During the exit conference held on October 14, 2021, OIG confirmed that HVAs lacking assessment were resolved in FY21. We request clarification in the final report to note that the assessments were completed by the Bureau upon notification by the Office of Inspector General (OIG) team.

The United States Patent and Trademark Office (USPTO)

General Comments

The United States Patent and Trademark Office (USPTO) appreciates the opportunity to review and comment on the OIG's draft report on the system security assessment process. USPTO reviewed the draft report and provided comments to Department of Commerce (DOC) Office of the Chief Information Officer (OCIO) for further discussions to ensure consistent implementation across the Department.

International Trade Administration (ITA)

General Comments

ITA concurs with the findings outlined in '*The Department Needs to Improve Its System Security Assessment and Continuous Monitoring Program to Ensure Security Controls Are Consistently Implemented and Effective*' (November 24, 2021). Additionally, in response to the report, ITA will implement the following:

- Conduct an assessment for its common controls package for the FY2022 year.
- Verify that assessment supporting documentation is maintained and sufficiently supports assessment results to facilitate oversight.
- Determine why Plan of Action and Milestones (POA&M) dates are not achievable (if not achievable).
- ITA has made POA&Ms better planned, prioritized, and resolved in a timely manner.
- Hold individuals accountable for not resolving issues within established milestones.
- Work to automate and customize Cyber Security Assessment and Management (CSAM) data entry to ensure CSAM accurately reflects bureau data.

National Oceanic and Atmospheric Administration (NOAA)

The National Oceanic and Atmospheric Administration appreciates the opportunity to review and comment on the OIG's draft report on the system security assessment process. NOAA reviewed the draft report and provided comments below.

General Comments

NOAA understands that gaps still exist regarding implementing the Risk Management Framework (RMF) across all systems within the Department of Commerce and NOAA will use this audit to improve NOAA's mature implementation to further enhance our security posture.

Recommended Changes for Factual/Technical Information

PDF Page 11 (Document Page 7), second paragraph, second sentence:
NOAA performs independent assessments of all Federal Information Security Modernization Act systems and the information provided as part of the audit reflects this.

PDF Page 11, (Document Page 7), second paragraph, third sentence:
NOAA also performs independent assessments of all of our high-value assets and the information provided as part of the audit reflects this.

U.S. Census Bureau (Census)

The Census Bureau appreciates the continued work of the Office of Inspector General in conducting transparent reviews and providing recommendations that have supported the Census Bureau and the broader Department of Commerce in maintaining and continuously improving cybersecurity methodologies and procedures.

Recommended Changes for Factual/Technical Information

Responses to Specific Sections of the Draft Report

Comments for Finding I: "The Department Did Not Effectively Plan for System Assessments"

The Census Bureau has no substantiative comments on this section. Since the period of evidence collection, the Census Bureau has taken steps to improve our planning process and documentation as discussed with OIG.

Comments on Finding II: "The Department Did Not Consistently Conduct Reliable System Assessments"

The Census Bureau concurs with the comments made by the OIG. The Census Bureau is committed to conducting accurate assessments and continues to make progress in our risk management activities, including initiating preassessment activities. Pre assessments are captured in our Governance, Risk, and Compliance tool, and demonstrate actions taken by Information System Security Officers (ISSOs), Security Engineers, and Assessment staff to plan and prepare prior to assessment kick-off.

Comments on Finding III: "The Department Did Not Resolve Security Control Deficiencies Within Defined Completion Dates"

The Census Bureau appreciates the work of the OIG in helping the Census Bureau to identify issues and provide support for the resolution. Since March 2021, the Office of Information Security (OIS) has led an initiative to review and closeout delayed POA&Ms, beginning with those most delayed and those categorized as "critical" priority level. As of December 2021, OIS has remediated all delayed "critical" and "high" POA&Ms. The Bureau concurs with recommendations 4, 5, and 6.

As the Census Bureau moves forward with its redesigned system plan, POA&Ms will be created and assigned at a control level instead of at a control test step level, reducing the reporting burden for staff. This directive serves to better align POA&M creation with substantive improvements and federal directives. Census has also established 'ground truth testing' capabilities that primarily leverage a dedicated, internal penetration testing team, further improving the situational awareness of current and emerging cyber-attack techniques, and simulating those activities in a safe manner to continuously confirm control effectiveness across the IT enterprise.

Comments on Finding IV: "The Department's Security System of Record—i.e., the CSAM Tool—Did Not Provide Accurate and Complete Assessment and POA&M Data"
The Census Bureau has no comments on this section and looks forward to partnering with the Department to implement recommendations 7 and 8.