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

September 14, 2022

MEMORANDUM FOR: Don Graves
Deputy Secretary of Commerce

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

SUBJECT: *Missing Security Controls Put the Department's Cloud-Based High Value Assets at Risk*
Final Report No. OIG-22-031-A

This final report provides the results of our audit of the U.S. Department of Commerce's (the Department's) security controls for cloud-based high value assets (HVAs). Our objective was to verify that the Department implemented security controls for cloud-based HVAs in accordance with federal requirements.

Overall, we found that the Department does not incorporate all customer responsibility controls for its cloud-based HVAs into system security plans (SSPs). This report includes a recommendation for the Department to include customer-defined controls in SSPs. See appendix A for specific details on our scope and methodology.

Introduction

The federal government has increased its efforts to modernize its approach to information technology (IT) by accelerating the adoption of cloud-based solutions. This effort has pushed aspects of IT security to the forefront, including securing HVAs that may now be available over the Internet. In prior audit work, we identified instances of mismanagement of security control implementation for both HVAs and cloud-based systems.[1] Proper security control selection is a foundational security step to protect systems and their data. Identifying and documenting necessary controls ensures they are implemented, assessed, and continuously verified throughout the system's life cycle. Observations from our prior work—coupled with the federal government's emphasis on agencies adopting cloud solutions—serve as the catalyst to focus this audit on security controls for cloud-based HVAs.

HVAs are information systems so critical to an organization that the loss or corruption of information or access would have serious impacts on the organization's ability to perform its

[1] U.S. Department of Commerce Office of Inspector General, January 25, 2022. *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. Washington, DC: DOC OIG, pgs. 24–25.

mission or conduct business.[2] As with any system, HVAs can rely on cloud services and, in turn, cloud service providers (CSPs). Management of cloud-based systems requires coordination between the CSP (e.g., Amazon GovCloud, Microsoft Azure, and Google Services) and the customer (e.g., the Department). This shared responsibility makes it imperative that both entities work in unison to ensure system data maintains its confidentiality, integrity, and availability.

All systems operated by or on behalf of the federal government are required to go through a series of steps to ensure that they are operating with an acceptable level of risk before they are authorized to operate. CSPs require this authorization independent of the customer agency's internal system. To carry out this process, agencies depend on the Federal Risk and Authorization Management Program (FedRAMP) to accredit and authorize CSPs for operation.[3]

Prior to FedRAMP accreditation, CSPs must establish a security control baseline that provides the minimum security control[4] requirements necessary to protect the system. These controls are then defined in a customer responsibility matrix (CRM), where they are designated as the responsibility of the (1) CSP, where the CSP provides the controls capability, (2) customer, where the customer (i.e., the Department) is responsible for implementing the control, or (3) CSP and customer, who both share the control's implementation.

Finding and Recommendation

The objective of this audit was to verify that the Department implemented security controls for cloud-based HVAs in accordance with federal requirements. Appendix A provides more details regarding our scope and methodology.

We found that the Department does not always incorporate security controls deemed necessary by the CSP for HVAs, putting the Department and its critical data at risk. Given the importance of HVAs to the Department's mission, it is vital to ensure all baseline security controls are incorporated into SSPs to prevent disruption.

The Department Does Not Incorporate All Customer Responsibility Controls for Its Cloud-Based HVAs into SSPs

In order for a FedRAMP system to be considered compliant, Department policy requires documentation of "[a]ny security controls needed for the use of the service which are not sufficiently provided by the CSP and how they are to be implemented and monitored, such

[2] *See* DOC National Institute of Standards and Technology Computer Security Resource Center. *High Value Asset (definition)* [online]. https://csrc.nist.gov/glossary/term/high_value_asset (accessed May 12, 2022).

[3] FedRAMP is a government-wide program that provides a standardized approach to security authorizations for cloud service offerings. *See* FedRAMP. *Program Basics* [online]. https://www.fedramp.gov/program-basics/ (accessed May 12, 2022).

[4] NIST describes a security control as "[a] safeguard or countermeasure prescribed for an information system or an organization designed to protect the confidentiality, integrity, and availability of its information and to meet a set of defined security requirements." DOC NIST CSRC. *Security control (definition)* [online]. https://csrc.nist.gov/glossary/term/security_control (accessed May 12, 2022).

as: 1) Agency responsible; 2) Hybrid; and 3) Optional controls selected by the bureau."[5] Further, Department policy[6] requires the documentation of all system security controls within the SSP. Due to the nature of cloud-based systems, security staff must consider both the Department- and CSP-defined baseline security controls when developing SSPs.

We reviewed the Department's nine[7] cloud-based HVAs to verify that all controls defined as "customer responsibility" by the CSP were included in the SSP. After comparing the customer responsibility matrix against the SSP, we found that four of the nine systems were missing implementation details for some assigned customer security controls (see table).

Table: Systems Missing Controls

System Name	Percent of Missing Controls
National Oceanic and Atmospheric Administration (NOAA) System 1	24 percent
United States Patent and Trademark Office (USPTO) System 1	11 percent
NOAA System 2	7 percent
NOAA System 3	3 percent

Source: Office of Inspector General analysis of security documentation

We found missing implementation details in important control areas such as access control, audit and accountability, and incident response that help prevent or reduce the impact of security incidents. Our testing noted that many of the missing controls exceeded the Department's standard control baseline. Although controls exceeded the Department's standards, CSP baselines are tailored specifically to fulfill the provider's system security needs as part of the FedRAMP authorization process. As such, it is crucial that the Department reviews and outlines the implementation status[8] for all controls the CSP deems necessary.

Based on interviews with bureau officials, we noted that there was no enterprise-wide process to ensure security staff reviewed and considered all customer-defined controls for implementation. The bureaus reported that although they reviewed customer responsibility matrices and added controls they considered necessary, they did not always record this process. Additionally, after review of the Department's FedRAMP policy, we determined that although it requires review of customer-defined controls, it does not provide sufficient guidance for documenting control implementation status.

[5] DOC, June 2019. *Department of Commerce Information Technology Security Baseline Policy (DOC ITSBP)*, Version 1.0. Washington, DC: DOC, Annex C-10: FedRAMP Applicability.

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

[7] See appendix A for more information about our system selection criteria.

[8] Control implementation status indicates whether the control is implemented, planned to be implemented, or not applicable.

The Department and CSP are only responsible for their respective controls; the CSP does not review or assess customer-defined responsibilities and vice versa. Both parties need to fulfill their responsibilities for the overall security of the system to be effective. Not including customer-defined controls in the SSP puts cloud-based HVAs at risk of missing controls needed to protect mission-critical data and operations. Without documented evidence that all customer-defined CSP controls have been reviewed, there is no assurance that the right controls were selected. If controls are not properly selected, they may not be implemented, assessed, and continuously verified, putting mission-critical HVAs at risk.

Recommendation

We recommend that the Deputy Secretary of Commerce direct the Department's Chief Information Officer to (1) revise Department policy to require that SSPs include the implementation status of customer-defined CSP baseline security controls on all cloud systems or document justification for not incorporating those controls, and (2) verify all cloud-based HVA SSPs comply with the revised policy.

Summary of Agency Response and OIG Comments

On August 18, 2022, we received the Department's response to our draft report. In response to our draft report, the Department generally concurred with our observations, finding, and recommendation and described actions it has taken, or will take, to address them. The Department's response included technical comments from NOAA and USPTO, which resulted in one change to the final report for clarification. The Department's and bureaus' formal responses are included within the final report as appendix B.

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

NOAA's Response

NOAA generally concurred with our observations and stated it has already taken proactive steps to address some of the identified issues. We appreciate NOAA's responsiveness in prioritizing the security of mission-critical HVAs. Additionally, NOAA provided technical comments related to missing control applicability and presence in other security documents. More specifically, it stated that *"[s]everal controls were not included in the FedRamp baseline for the cloud service and are not applicable" and* that some missing controls were in other security documents (such as a newer version of the SSP).

OIG Comment

During fieldwork, we identified missing security controls to NOAA's system security staff. We worked with NOAA to resolve differences, the results of which were reflected in the draft report. Regarding NOAA's assertion that several controls were not applicable, we derived the requirements directly from the Department and CSP FedRAMP security control baseline for each specific system. Additionally, while NOAA provided us with an updated SSP, the document was dated after we notified NOAA of the errors and was not in effect at the time of our testing.

USPTO's Response

USPTO stated that missing controls were *". . . addressed via a reference to a valid hosting system that documents customer responsibility" and "[t]he assertion that required controls are missing or unselected for USPTO System 1 is not fully accurate."*

OIG Comment

While we recognize that USPTO does have a common control provider (i.e., hosting system), our testing determined that the references to that system were not specific enough to identify what controls were applicable and how they were being inherited for the specific system we tested. It is important that USPTO identify and document applicable controls within each system's SSP, as required by Department policy.

Pursuant to Department Administrative Order 213-5, please submit to us an action plan that addresses the recommendation 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) 793-2938 or Chuck Mitchell, Director for Cybersecurity, at (202) 809-9528.

cc: André Mendes, Chief Information Officer, OCIO
Zachary Goldstein, Chief Information Officer, NOAA
Jamie Holcombe, Chief Information Officer, USPTO
Ryan Higgins, Chief Information Security Officer, OCIO
Joselyn Bingham, Audit Liaison, OCIO
Maria Hishikawa, IT Audit Liaison, OCIO
MaryAnn Mausser, Audit Liaison, Office of the Secretary

Appendix A.
Objective, Scope, and Methodology

Our audit objective was to verify that the Department implemented security controls for cloud-based HVAs in accordance with federal requirements. To accomplish our objective, we did the following:

- Analyzed the nine systems that matched our criteria of operational HVAs with external cloud providers throughout the Department:
  - Reviewed documentation from the Department and FedRAMP for each system's representative CSP to identify the Department's customer responsibilities.
  - Established our criteria based on the Department's *ITSBP* and CSP customer responsibility requirements.
  - Assessed system security documentation provided by bureaus or collected from the cyber security asset and management tool to verify customer security control responsibilities were included.
- Interviewed Department officials from several bureaus responsible for developing SSPs and managing cloud-based IT systems.

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

- The Department's *ITSBP*
- National Institute of Standards and Technology (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*

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.*[9]

The following security control as defined in the *ITSBP* and NIST *Special Publication 800-53* was significant to our audit objective:

> *PL-2 System Security Plans* – We identified issues with the implementation of these security controls as described in the Finding and Recommendation section of this report.

[9] U.S. Government Accountability Office, September 2014. *Standards for Internal Control in the Federal Government*, GAO-14-704G. Washington DC: GAO. Available online at https://www.gao.gov/assets/gao-14-704g.pdf (accessed May 26, 2022).

Our analysis did not rely on computer-processed data to support our finding, conclusion, or recommendation.

We conducted our review from January 2022 through April 2022 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 finding and conclusion based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our finding and conclusion based on our audit objective.

Appendix B.
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: 2022.08.17 12:29:36 -04'00'

SUBJECT: Department of Commerce's Concurrence to the Inspector General's Draft Report, *Missing Security Controls Put the Department's Cloud-Based High Value Assets at Risk* (OIG-22-418, July 19, 2022)

We appreciate that the Office of the Inspector General (OIG) presented the Department of Commerce (DOC) with an opportunity to review the Draft Report, *Missing Security Controls Put the Department's Cloud-Based High Value Assets at Risk (OIG-22-418, July 19, 2022).*

The DOC Office of Chief Information Officer (OCIO) has reviewed the draft report and generally concurs with the finding and recommendation. The DOC OCIO is prepared to issue new Enterprise Cybersecurity Policy and the Security and Privacy Control Baseline, upon completion of internal review processes. The Office of Cybersecurity and IT Risk Management (OCRM) conducts monthly reviews of system security plans and associated artifacts to ensure compliance with published policy. 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
- FY 2022 Q4 OIG-22-418 DOC Formal Comments to Draft Report

cc: MaryAnn Mausser, DOC
Joselyn Bingham, Audit Liaison, DOC
Ryan Higgins, Chief Information Security Officer, DOC
Maria Hishikawa, IT Audit Liaison, DOC

Department of Commerce Technical and Editorial Comments on the OIG Draft Report entitled, ***Missing Security Controls Put the Department's Cloud-Based High Value Assets at Risk (OIG-22-418, July 19, 2022)***

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.

National Oceanic and Atmospheric Administration (NOAA)

General Comments

NOAA appreciates the thorough assessment performed on the High-Value Assets utilizing cloud-based services and do not disagree with the findings. However, we would like to reassert the comments that were provided to the OIG as part of follow-up questions we addressed.

For NOAA labeled system 1, POA&M 11747 has been created to address several controls that were not documented in the SSP. This POA&M is being monitored and tracked by NOAA's OCIO/CSD with updates being briefed to the Authorizing Official quarterly. Several controls were not included in the FedRamp baseline for the cloud service and are not applicable. Other controls were documented in the system's FIPS 200 as not applicable, and the Authorizing Official approved this document. Lastly, several controls are common within the NOAA enterprise and are documented as such in the system security plan.

For the NOAA system labeled system 2, the current system security plan is currently being reviewed and updated to address all controls listed as not implemented in the assessment.

For NOAA system labeled system 3, several controls are provided by the NOAA CASB solution and were found to be satisfied in the FY21 assessment of the system. Additionally, this system has migrated to a NIST 800-53 rev 5 baseline and several controls have been combined in the new baseline provided by NIST.

The above clarifications should be considered prior to issuing the final report given the systems in question are managing the risk posed by utilizing cloud-based services within the HVA system boundary.

The United States Patent and Trademark Office (USPTO)

Page 2, Paragraph 5, Sentence 1: *"We found that the Department does not always incorporate security controls deemed necessary by the CSP for HVAs, putting the Department and its critical data at risk."* In the case of USPTO System 1 (i.e., the Fee Processing Next Generation System (FPNG)), all required security controls are incorporated in the Cloud HVA's baseline and are fully implemented. They are addressed via the reference to the USPTO Amazon Web Services Cloud Services (UACS) System Security and Privacy Plan (SSPP) in the FPNG SSPP. UACS is the USPTO's vehicle for implementing the Amazon Web Services (AWS) U.S. East (Northern

Virginia)/West (Oregon) Regions Cloud Service Provider (CSP), and the UACS SSPP addresses the "customer responsibility" requirements for all the required controls.

Page 3, Paragraph 3, Sentences 1 and 2: *"We found missing controls from important areas such as access control, audit and accountability, and incident response that help prevent or reduce the impact of security incidents. Our testing noted that many of the missing controls exceeded the Department's standard control baseline."* As noted above, the "11 percent" of controls cited in the finding for USPTO System 1 is addressed via a reference to the USPTO UACS System in the FPNG SSPP. UACS serves as the control implementation vehicle for the AWS U.S. East/West Regions CSP and provides the implementation status and details for all customer responsibility controls for USPTO systems hosted in AWS. As a result, referring to these controls as "missing" for USPTO System 1 is not fully accurate. The controls are implemented and addressed via a valid reference to UACS, which documents the customer responsibility portion for all required controls.

Page 4, Paragraph 1, Sentences 1-3: *"Not including customer-defined controls in the SSP puts cloud-based HVAs at risk of missing controls needed to protect mission-critical data and operations. Without documented evidence that all customer-defined CSP controls have been reviewed, there is no assurance that the right controls were selected. If controls are not properly selected, they may not be implemented, assessed, and continuously verified, putting mission-critical HVAs at risk."* As noted above, all required controls have been properly selected and are implemented and documented via the UACS control provider relationship, which is documented in the FPNG SSPP. The report, as it pertains to USPTO System 1, should be updated to reflect that the controls are addressed via a reference to a valid hosting system that documents the customer responsibility portion for all controls required by the CSP. The assertion that required controls are missing or unselected for USPTO System 1 is not fully accurate.