~~CONTROLLED UNCLASSIFED INFORMATION (CUI) // SPECIFIED SENSITIVE SECURITY INFORMATION (SP-SSI)~~

OST

Redacted Final Report
No. IT2024001
October 30, 2023

DOT Needs To Improve Its High-Value Assets Governance Program To Effectively Identify, Prioritize, and Secure Its Most Critical Systems

~~WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.~~

DOT Needs To Improve Its High-Value Assets Governance Program To Effectively Identify, Prioritize, and Secure Its Most Critical Systems

Self-initiated

Office of the Secretary of Transportation | IT2024001 | October 30, 2023

What We Looked At

High value assets (HVA) are information systems, information, and data for which unauthorized access, use, disclosure, disruption, modification, or destruction could have a significant impact on U.S. national security, or public health and safety of the American people. Given the impact that cyberattacks on HVAs can have on the security and resilience of the Nation's transportation infrastructure, we initiated this audit of DOT's HVA Program. At the time of our review, DOT identified that it had [redacted] HVAs. Our objectives were to evaluate whether DOT (1) established an organization-wide HVA governance program to identify and prioritize HVAs and (2) assesses HVA security controls and ensures timely remediation of identified vulnerabilities.

What We Found

DOT has not established an effective HVA governance program for identifying, prioritizing, and securing its most critical information and information systems because the Department did not consistently follow Federal requirements to address significant risks to HVAs. DOT's Chief Information Security Officer (CISO) in place at the time of our review stated the Department's HVA governance program has been managed and operated in an ad hoc and inconsistent manner across the organization and does not account for all the risks to its HVAs. DOT also lacks an assessment approach, timely remediation of weaknesses, and effective incident response plans for its HVAs. The inability to appropriately mitigate and remediate persistent HVA-related cybersecurity weaknesses in a timely manner poses a major risk to the Department's efforts to adequately protect its most critical information and information systems.

Our Recommendations

We made seven recommendations to strengthen DOT's HVA Program cybersecurity. DOT concurred with five recommendations and did not concur with and asked to close the other two recommendations. We consider the five recommendations resolved but open pending completion of planned corrective actions. We consider the remaining two recommendations unresolved and request that DOT provide an updated response, reconsider its non-concurrence, or provide documentation to support closing the recommendations.

~~***WARNING:*** **This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.**~~

All OIG audit reports are available on our website at www.oig.dot.gov.

For inquiries about this report, please contact our Office of Government and Public Affairs at (202) 366-8751.

Contents

Memorandum 1

Results in Brief 3

Background 5

DOT Has Not Established an Effective High Value Assets Governance Program for Identifying and Prioritizing Its Most Critical Systems 7

DOT Lacks an Assessment Approach, Timely Remediation of Weaknesses, and Effective Incident Response Plans for Its High Value Assets 16

Conclusion 28

Recommendations 28

Agency Comments and OIG Response 30

Actions Required 30

Exhibit A. Scope and Methodology 31

Exhibit B. Organizations Visited or Contacted 33

Exhibit C. List of Acronyms 34

Exhibit D. Major Contributors to This Report 37

Appendix. Agency Comments 38

U. S. Department of Transportation
Office of Inspector General

Memorandum

Date: October 30, 2023

Subject: ACTION: DOT Needs To Improve Its High-Value Assets Governance Program To Effectively Identify, Prioritize, and Secure Its Most Critical Systems| Report No. IT2024001

From: Kevin Dorsey
Assistant Inspector General for Information Technology Audits

To: Chief Information Officer

High value assets (HVA) are information systems, information, and data for which unauthorized access, use, disclosure, disruption, modification, or destruction could have a significant impact on U.S. national security and economic interests, foreign relations, public confidence, civil liberties, or public health and safety of the American people.[1] The Department of Transportation (DOT) identified [redacted] HVAs at the time of our review.

HVAs enable mission-essential functions (MEF) and operations, which must be continued or resumed rapidly after a disruption of normal operations. MEFs are the backbone of continuity planning and cannot be deferred during an emergency or disaster. HVAs are so critical their loss or corruption could impact DOT's ability to perform the following primary mission-essential functions (PMEF):

- Assure the operation, availability, and safety of critical transportation systems and infrastructure necessary for national defense;
- Lead and coordinate the national response to significant disruption to the transportation sector; and

[1] Office of Management and Budget (OMB) Memorandum M-17-09, *Management of Federal High Value Assets,* December 9, 2016.

- Ensure the continuous operation of the National Airspace System (NAS) and maintain critical air services and safety.

HVAs may contain sensitive controls, instructions, or data used in critical operations, which make them of particular interest to criminal, politically motivated, or state-sponsored actors seeking to exploit the data or cause a loss of public confidence. Given the impact that cyberattacks can have on the security and resilience of the Nation's transportation infrastructure, we initiated this audit of DOT's HVA Program. Our objectives were to evaluate whether DOT (1) established an organization-wide HVA governance program to identify and prioritize HVAs and (2) assesses HVA security controls and ensures timely remediation of identified vulnerabilities.

To conduct our work, we interviewed HVA officials from DOT and the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA). We issued data calls to DOT's 11 components[2] and collected and analyzed Security Controls Authorization Packages for DOT's designated HVAs. We also reviewed policies and procedures directing Federal agencies to identify, prioritize, and secure HVAs.

We conducted this audit in accordance with generally accepted Government auditing standards (GAGAS). Exhibit A details our scope and methodology. Exhibit B lists the organizations we visited or contacted, and exhibit C lists the acronyms used in this report.

We appreciate the courtesies and cooperation of DOT representatives during this audit. If you have any questions concerning this report, please contact me or Leon Lucas, Program Director.

cc: DOT Audit Liaison, M-1

[2] Component has the meaning established in DOT Order 1351.A, IT Policy Management, and refers to all DOT Operating Administrations, the Office of the Secretary of Transportation, and the Office of the Inspector General.

Results in Brief

DOT has not established an effective high value assets governance program for identifying and prioritizing its most critical systems.

DOT's Office of the Chief Information Officer (OCIO) did not consistently follow OMB guidance[3] or CISA's recommended actions to address significant risks to the Department's HVAs. For example, OCIO did not establish an organization-wide HVA governance program with an office, team, or other governance structure, including specific policies and procedures for identifying and prioritizing HVAs. While, for the most part, OCIO identified and prioritized [redacted] HVA information systems, OCIO did not provide any evidence that the [redacted] remaining HVAs met OMB or CISA criteria to: (1) provide informational value, (2) provide MEFs, or (3) serve a critical function of the Federal civilian enterprise. OCIO also did not identify the interconnectivity, dependencies, criticality, or mission importance of these seven information systems to determine whether they should have been considered for designation as HVAs. Further, among the [redacted] verified HVAs, OCIO officials did not provide evidence that they had considered the interconnectivity and dependencies for [redacted] of them or identified the criticality and mission importance for [redacted] of the [redacted]. We interviewed OCIO officials, including the Department's Chief Information Security Officer (CISO) in place at the time of our review, who stated the DOT HVA governance program has been managed and operated in an ad hoc and inconsistent manner across the organization and does not account for all the risks to its HVAs. The lack of an effective organization-wide governance program to properly identify, prioritize, and secure its most critical information and information systems puts DOT at a major risk of failing to achieve the OMB cybersecurity strategy for protecting HVAs from cyber-incidents and ensuring robust physical and cybersecurity protections are in place.

[3] OMB M-19-03, *Strengthening the Cybersecurity of Federal Agencies by Enhancing the High Value Asset Program*, December 10, 2018.

DOT lacks an assessment approach, timely remediation of weaknesses, and effective incident response plans for its high value assets.

OCIO did not develop an assessment approach for the [redacted] HVAs we identified[4] at the time of our review that, per CISA requirements, should be designed to identify and prioritize HVA risks and weaknesses for timely mitigation and architectural enhancement. OCIO officials with whom we spoke acknowledged that this is the case. Moreover, OCIO does not consistently ensure timely remediation of identified vulnerabilities to address significant risks to its HVAs. According to OCIO officials, they instead rely on assessments and reviews performed by DHS, as well as internal Federal Information Security Modernization Act (FISMA)[5] reviews to assess security weaknesses for DOT's HVA systems. DHS assessed 2 of DOT's [redacted] designated HVAs for risks and weaknesses and was able to exploit some vulnerabilities and gain unauthorized access into both HVAs. DOT officials have yet to fully remediate the DHS findings. We assessed the remaining [redacted] HVAs and found that DOT was not performing annual security control assessments for [redacted] of them as FISMA requires, ensuring timely remediation of security control weaknesses for any of the [redacted] systems, or updating privacy documents for the [redacted] HVAs to adequately protect sensitive or personally identifiable information (PII). Furthermore, DOT did not properly test the contingency and incident-handling activities in accordance with CISA requirements for [redacted] of the [redacted] HVAs to determine if they could recover from a disruption of normal operations within established timeframes. Additionally, DOT officials did not provide adequate supporting documentation for our office to assess the remaining four HVAs. DOT HVA officials attributed the Department's inability to perform annual assessments and remediate weaknesses to limited or a lack of adequate resources. However, the inability to appropriately mitigate and remediate persistent HVA-related cybersecurity weaknesses in a timely manner poses a major risk to the Department's efforts to adequately protect its most critical information and information systems. Also, the loss or corruption of HVAs can impact DOT's ability to perform its PMEFs, which would have an impact on national defense, the nationwide transportation sector, and the NAS.

[4] For the purpose of our review, we determined whether DOT assessed HVA security controls and ensured its identified vulnerabilities were remediated timely for only [redacted] HVAs. We concluded DOT, for the most part, followed CISA criteria for designating the [redacted] HVAs, but we did not assess the remaining [redacted] because DOT did not follow CISA requirements.

[5] Public Law Number (Pub. L. No. 113-283) (2014). FISMA requires agencies to report the status of their information security programs to OMB annually.

We made seven recommendations to improve DOT's HVA governance program and ability to remediate identified security vulnerabilities in a timely manner.

Background

Since 2015, the Federal Government's HVA initiative[6] has focused on protecting the most critical and high-impact information and information systems. This broad Government effort and its related policy statements address the identification, categorization, and prioritization of HVAs in all Federal agencies. In addition, Federal agencies are required to report their HVAs to DHS annually and establish appropriate protections to improve HVA security postures. Specifically, in its 2015 *Cybersecurity Strategy and Implementation Plan*, the Office of Management and Budget (OMB) asked agencies to "identify their HVAs and critical system architecture in order to understand the potential impact to those assets from a cyber-incident and ensure robust physical and cybersecurity[7] protections are in place." These activities focus on the identification of major and critical weaknesses to HVA systems through tailored assessments conducted by DHS, the agency, or an independent third-party assessor in accordance with Governmentwide requirements.

OMB's Memorandum M-19-03, *Strengthening the Cybersecurity of Federal Agencies by Enhancing the High Value Asset Program* (2018), consolidated and updated previous OMB requirements[8] on HVA identification, assessment, remediation, and response to incidents. The memorandum provides guidance on DHS's operation of the HVA program in coordination with OMB. It outlines expectations in the following six areas: (1) establishing an enterprise HVA governance program; (2) improving the designation of HVAs; (3) implementing data-driven HVA prioritization; (4) increasing the trustworthiness[9] of HVAs; (5) protecting privacy and HVAs; and (6) defining HVA reporting, assessment, and remediation requirements. The memorandum also provides a more flexible approach for identifying HVAs; rather than relying on a single definition, it allows

[6] DHS Binding Operational Directive (BOD) 18-02, *Securing High Value Assets*, 2018.

[7] Cybersecurity is the ability to protect or defend the use of cyberspace from cyberattacks.

[8] OMB Memorandum M-17-09, *Management of Federal High Value Assets*, December 9, 2016.

[9] OMB Circular A-130, *Managing Information as a Strategic Resource*, July 28, 2016, defines a "trustworthy information system" as one that is believed to be capable of operating within defined levels of risk despite the environmental disruptions, human errors, structural failures, and purposeful attacks that are expected to occur in its environment of operations.

agencies to designate Federal information or information systems based on their relation to one or more of the following categories:

- **Informational Value** – The information or information system that processes, stores, or transmits the information is of high value to the Government or its adversaries.
- **Mission Essential** – The agency cannot accomplish its PMEFs—as approved in accordance with Presidential Policy Directive 40 (PPD-40),[10] the National Continuity Policy—within expected timelines without the information or information system.
- **Federal Civilian Enterprise Essential (FCEE)** – The information or information system serves a critical function in maintaining the security and resilience of the Federal civilian enterprise.

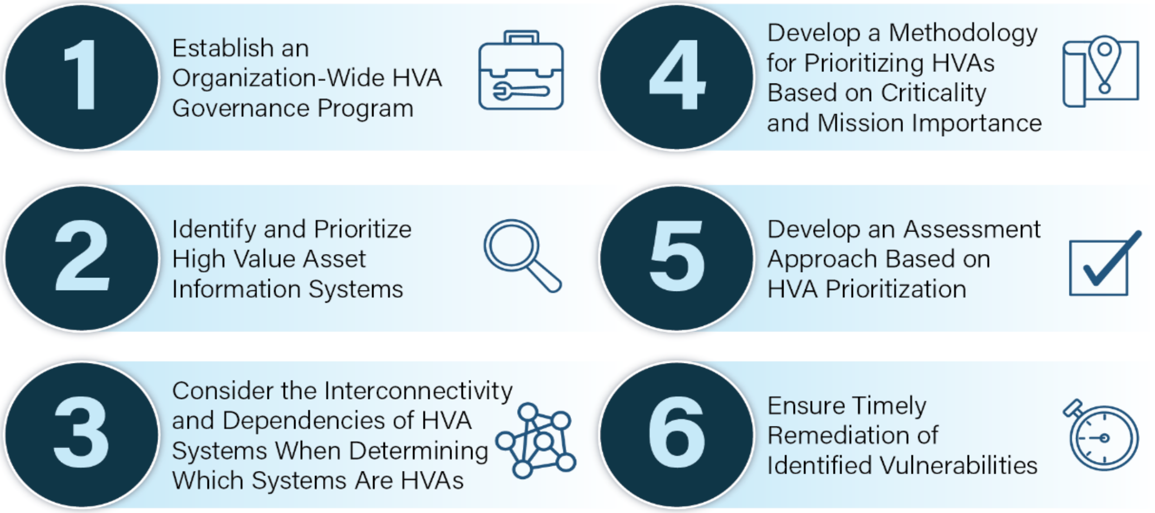
According to M-19-03, while agencies are principally responsible for designating HVAs, OMB and DHS may also designate HVAs at agencies based on the potential impact to national security.

Moreover, to address the significant risks to HVAs, CISA directed Federal civilian agencies to undertake a series of recommended actions, which are outlined in *CISA Insights on Securing High Value Assets*[11] (see figure 1):

[10] Presidential Policy Directive 40 (PPD-40), *National Continuity Policy*, July 15, 2016, directs coordination of implementation, execution, and assessment of continuity activities among executive departments and agencies.

[11] CISA Insights: Secure High Value Assets (HVAs).

Figure 1. CISA-Recommended Actions for Securing High Value Assets



1 Establish an Organization-Wide HVA Governance Program

2 Identify and Prioritize High Value Asset Information Systems

3 Consider the Interconnectivity and Dependencies of HVA Systems When Determining Which Systems Are HVAs

4 Develop a Methodology for Prioritizing HVAs Based on Criticality and Mission Importance

5 Develop an Assessment Approach Based on HVA Prioritization

6 Ensure Timely Remediation of Identified Vulnerabilities

Source: CISA

Overall, the recommended actions address the identification, categorization, and prioritization of HVAs and focus on an assessment approach to identify and prioritize risks and weaknesses for timely mitigation and develop architectural enhancements based on the assessment results.

DOT Has Not Established an Effective High Value Assets Governance Program for Identifying and Prioritizing Its Most Critical Systems

Although OMB and CISA provide specific criteria for establishing an HVA governance program, the Department has managed its HVA governance program in an ad hoc and inconsistent manner across the organization. Furthermore, DOT has not established an effective process for identifying and prioritizing its HVAs, consistently considered the interconnectivity and dependencies of its HVA systems, or developed a methodology for prioritizing HVAs based on criticality and mission importance. As a result, the Department's program is not effective.

DOT Manages Its HVA Governance Program in an Ad Hoc Manner

In coordination with OMB, CISA directed Federal agencies to establish an organization-wide HVA governance program as a first step in securing their HVAs. CISA directed organizations to take a strategic, enterprise-wide view of cyber risk that unifies the effort to protect HVAs against evolving cyber threats. However, DOT's HVA governance program lacks structure and consistency and has not followed some CISA requirements, raising questions about whether the Department is prepared to address cyber risks facing its most critical systems. Specifically:

- DOT has identified an HVA Lead responsible for coordinating the Department's HVA assessments with DHS. However, it has not established an office, team, or other governance structure, including policies and procedures, as CISA recommends for effective HVA governance programs.
- Contrary to CISA's recommendations, DOT does not have a governance structure that incorporates HVA activities (e.g., assessment, remediation, and incident response) into broader planning activities for information system security and privacy management. Furthermore, DOT has not included HVA activities in its broader planning documents, such as those focused on enterprise risk management and contingency planning.
- In interviews we conducted to understand these shortcomings, DOT's CISO in place at the time of our review acknowledged that DOT's HVA program has been managed in an ad hoc and inconsistent manner across the organization and does not account for all the risks to its most valuable assets. Furthermore, according to OCIO officials, the program has not been fully implemented due to a lack of resources for this work because identifying HVAs and providing specific continued support is very labor intensive.

Without an established governance program, DOT will be significantly challenged to take a strategic, enterprise-wide view of the cyber risks facing its HVAs. Moreover, DOT officials may not be able to properly identify and prioritize the Department's most critical assets, adequately protect them, appropriately mitigate risks, or respond to an incident that occurs because the HVA governance program is not effective.

DOT Has Not Effectively Identified and Prioritized Its High Value Assets

DOT did not consistently follow CISA's and OMB's recommended approach when identifying and designating its HVAs. Also, the Department did not always consider the interconnectivity and dependencies of its HVA systems when it determined which systems were HVAs. Finally, DOT did not consistently follow a methodology for prioritizing HVAs based on criticality and mission importance. Consequently, DOT lacks an effective program to properly identify, prioritize, and designate its most critical information and information systems as HVAs. As a result, the Department faces the major risk of failing to meet OMB's cybersecurity strategy for protecting those assets from cyber-incidents and ensuring that robust physical and cybersecurity protections are in place.

DOT Lacks an Effective Process for Identifying and Prioritizing Its HVA Systems

OCIO did not consistently follow CISA's and OMB's recommended approach for Federal agencies that want to identify and designate information and information systems as HVAs. In April 2019, OCIO sent out a data call asking the components and OAs to identify their systems based on one or more of three categories: (1) informational value, (2) MEF, and (3) critical function as an FCEE system. OCIO also asked the OAs to provide other information pertaining to CISA's recommended actions for securing HVAs, including the systems' interconnectivity and dependencies, criticality, and mission importance. While the components and OAs identified [redacted] systems that, for the most part, met the criteria for identifying its information systems as potential HVAs, OCIO only designated [redacted] of them as HVA systems (see table 1). Moreover, OCIO designated [redacted] of the [redacted] systems as HVAs beyond those identified by OAs.

[redacted]

[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

Source: OIG analysis of OCIO data

To understand the discrepancies between OA and OCIO numbers, we asked officials from the 11 OAs to tell us the criteria they used to identify systems as potential HVAs in response to OCIO's data call. We found that 9 of the 11 officials were unable to do so clearly; FAA and FTA representatives were the exceptions. According to OA officials, DOT no longer employs some of the individuals who worked on HVA input, so they were not available to share their reasoning with us.

In addition, OCIO could not provide a rationale or supporting documentation for its decision to identify [redacted] OA-specific information or information systems as HVAs. As a result, neither the OAs nor OCIO could explain their differences of opinion about what counts as an HVA. Specifically:

- FAA identified [redacted] information systems that provide informational value, MEFs, and/or a critical FCEE function. However, OCIO only designated 6 of the [redacted] systems as HVAs. Although FAA reported [redacted] as high-impact information systems and a compromise the systems could have a severe impact on FAA's mission.

- FTA identified two information systems as providing MEFs, yet OCIO did not designate either as HVAs. [redacted]

- OST identified [redacted] information systems, but DOT only designated [redacted] as HVAs. One system DOT designated as an HVA—[redacted] was not among the [redacted] systems OST identified. This raises questions about why DOT designated CASTLE as an HVA when OST did not include it as one of the [redacted].

- The GLS security manager told us that the OA did not identify any systems and wasn't aware that OCIO designated its [redacted] as an HVA. This raises questions about OAs' ability to understand what constitutes an HVA. Moreover, DOT does not have jurisdiction over GLS IT system, which is a Canadian asset, nor track GLS's system in the Department's cybersecurity inventory system of record. This raises additional questions about OCIO's process for designating HVAs.

As required, OCIO reported its prioritized list of [redacted] HVAs through the Homeland Security Information Network; see table 2. (For descriptions of many of these system assets, see the next section of this report.)

[redacted]

[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]

DOT HVA Systems	Function Category	Interconnectivity/ Dependencies	Criticality/Mission Importance
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]

Source: DOT OCIO

However, in formulating its prioritized list, OCIO did not follow OMB's and CISA's recommended actions for designating [redacted] of those [redacted] systems as HVAs. Those seven systems are:

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

Specifically, the OAs did not identify whether their information systems provide informational value, MEFs, or a critical FCEE function, as CISA recommends, but

OCIO still designated the systems as HVAs without documenting any basis for determining the systems met these standards. Additionally, the OAs did not identify their systems' interconnectivity, dependencies, criticality, or mission importance; however, OCIO still designated the systems as HVAs.

For the most part, OCIO did follow OMB and CISA recommended actions for the remaining [redacted] HVA information systems. Those [redacted] systems are:

[redacted]

~~***WARNING:*** **This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.**~~

OCIO received information based on OAs response to the data call and provided evidence that the [redacted] HVAs provided informational value, MEFs, or a critical FCEE function. OCIO also identified the interconnectivity and dependencies for all but [redacted] of the [redacted] HVAs. Those three systems are:

- [redacted]
- [redacted]
- [redacted]

Also, OCIO identified the criticality and mission importance for all but [redacted] of the [redacted]. [redacted].

CISA states Agency HVA Points of Contact (POC) should consider whether saving the information they have collected for each HVA would be valuable. CISA reported this information could help Agency HVA POCs understand why an asset was or was not identified as an HVA in a given year, track HVAs, and articulate the reasons for changes in designation. However, OCIO did not have evidence documenting its decisions to identify and designate DOT HVAs. Maintaining such knowledge is critical to the process of identifying, prioritizing, and securing critical systems. Yet OCIO officials stated that they did not keep the OAs' informational spreadsheets after they developed the list of [redacted] HVAs for reporting purposes. DOT also could not provide us with evidence that it followed CISA's recommendation to review the HVA list quarterly, update it, or participate in the annual meeting DHS coordinates to validate Federal HVA lists. Absent such documentation, OCIO is unable to demonstrate that it complied with OMB or CISA recommended actions or that it applied due diligence to the critical process of identifying, prioritizing, and designating its most critical systems as HVAs.

In addition, neglecting to consider the functionality of dependent and interdependent systems can impact an HVA's operations and ability to perform its mission. Thus, CISA recommends that dependent and interdependent systems receive the same level of protection as primary HVA systems. Moreover, DOT's failure to develop a methodology to prioritize its HVAs based on criticality and mission importance raises questions about the accuracy of its designation of the [redacted] HVAs. We also found that DOT is not using its HVA list to prioritize monitoring for assessments and contingency actions across the Department's operational structure. Finally, DOT did not provide any evidence to show that the most important systems receive the highest priority of support, funding, and operations to fulfill the mission.

Overall, DOT has not implemented a data-driven prioritization for its HVA program and has failed to document the current processes. As a result, the Department may not be able to efficiently prioritize and allocate resources for its system assets, ensure their protection, and provide OMB and CISA with the required visibility into its HVAs.

DOT Lacks an Assessment Approach, Timely Remediation of Weaknesses, and Effective Incident Response Plans for Its High Value Assets

Rather than develop an assessment approach based on HVA prioritization that follows DHS assessment requirements, the Department relies on DHS and FISMA reviews to assess and identify weaknesses in its HVA systems. In addition, DOT does not remediate the HVA vulnerabilities it identifies in a timely manner. Further, DOT's contingency planning and incident handling activities are insufficient to support the Department's PMEFs should HVA operations be disrupted.

The Department Has Not Established an Assessment Approach for Its HVAs

According to CISA guidance, DOT should develop an assessment approach for its HVAs based on the Department's prioritization and management's appetite for risk tolerance. The HVA activities should focus on identifying major and critical weaknesses to HVA systems through tailored assessments provided directly by DHS, the agency, or an independent third-party assessor based on Governmentwide requirements. CISA recommends that agencies perform a tailored assessment, which can include a penetration test, of their HVAs at least once every 3 years to ensure the systems and information are protected at the appropriate levels commensurate with risks. DOT's HVA POC is responsible for ensuring the Department's HVAs receive the proper assessments and working with DHS to ensure HVA weaknesses are prioritized for timely mitigation and architectural enhancements based on the assessment results.

OCIO officials acknowledged the Department has not developed an assessment approach that adheres to the CISA guidance. They stated that the Department relies on DHS assessments and its FISMA reviews to assess and identify weaknesses in its HVA systems. For the [redacted] information systems our audit covers, we reviewed the DHS-led assessments for [redacted] HVAs and the Department internal FISMA reviews for [redacted] HVAs.

DOT Does Not Ensure Timely Remediation of HVA Vulnerabilities and Is Not Updating Privacy Documents

DOT is not consistently mitigating or remediating the HVA weaknesses identified through its DHS-led or FISMA assessments in a timely manner. Additionally, DOT is not updating its HVA privacy documents annually as required.

DHS Assessments of [redacted] DOT HVAs

DHS performs Security Architecture Reviews and Risk and Vulnerability Assessments of Federal agency HVAs. A Security Architecture Review is not a direct assessment of the HVA; it consists of a system documentation review and analysis, structured interviews, and tabletop exercises. It is designed to identify and assess business risks, security controls, and operational effectiveness. A Risk and Vulnerability Assessment is a direct assessment of the HVA, during which DHS performs penetration-testing scenarios with the intent of gaining access to sensitive data protected by the target HVA.

DHS performed several assessments on [redacted] of the Department's HVAs, but [redacted] of those systems—[redacted] did not appear on DOT's HVA list at the time of our review. CISA guidelines state that removing an asset from the HVA list requires a signed memo from the agency's Senior Accountable Official for Risk Management that specifies the change. However, OCIO officials did not provide any evidence that they followed this requirement. (These [redacted] assets are discussed in greater detail below.)

We reviewed the status of the [redacted] HVA systems that DHS assessed and are still on DOT's HVA list: [redacted]. We found the following:

- [redacted] DHS assessed [redacted] twice.

  - First, in May 2019, DHS completed a Risk and Vulnerability Assessment of [redacted]

  - Second, in September 2019, DHS completed a Security Architecture Review of [redacted]. DHS reported the following:

    - [redacted]
    - [redacted]
    - [redacted]

- [redacted]

  - In September 2016, DHS completed a Risk and Vulnerability Assessment of NPMS. DHS gained unauthorized access to an [redacted] remediate findings associated with weak password policy, elevated [redacted] PHMSA did not submit a remediation plan to DHS. [redacted]

- In February 2017, DHS released a draft Security Architecture Review of [redacted]. DHS made two recommendations to PHMSA: [redacted]

For the remaining [redacted] DHS-led assessments of HVAs that were removed from DOT's HVA list, we found the following.

- [redacted]
  - In September 2016, DHS completed a Risk and Vulnerability Assessment of the [redacted] DHS [redacted] However, OST did not submit a remediation plan to DHS. OST officials informed OIG that they [redacted]. We assessed OST's [redacted] as part of our FISMA review (see below).
- [redacted]
  - In May 2018, DHS completed a Security Architecture Review of [redacted]

[12] Spear phishing is a technique whereby emails that appear genuine are sent to all the employees or members within a certain company, Government agency, organization, or group.

[redacted] However, DHS concluded that [redacted]

DOT FISMA Assessments of [redacted]

According to OMB,[13] all Federal agencies are responsible for conducting ongoing authorization of their information systems; the goal is to ensure the accuracy of information pertaining to the security and privacy posture of their HVAs. However, based on our review of DOT's internal FISMA assessments of the remaining [redacted] we reviewed, DOT does not always conduct annual assessments or remediate cybersecurity weaknesses and system flaws in a timely manner. To assess DOT's compliance with the OMB guidelines for FISMA, we assessed whether the Department was effectively implementing security controls to protect its HVAs from compromise and prevent unauthorized access to sensitive security information. We found that DOT did not perform annual assessments, as FISMA requires, for [redacted] we examined. Additionally, DOT has not consistently ensured that its HVA vulnerabilities are mitigated in a timely manner. While DOT reports it is developing remediation plans to correct the weaknesses, the timelines and mitigation actions necessary to address certain vulnerabilities are either missing or delayed. According to DOT officials, the Department is in the process of adding resources to ensure the timely remediation of weaknesses.

- [redacted] serves as the primary telecommunications service provider for all FAA systems, both NAS and non-NAS (mission support). FAA performs annual security assessments and authorization for the FTI but does not ensure timely remediation of weaknesses. [redacted]

[13] OMB M-19-03.

[redacted]

- [redacted] provides services to FAA and the aviation community; those services include [redacted]
- [redacted] is a [redacted] to FAA. The Agency performs annual security assessments and authorization for the [redacted] but does not ensure timely remediation of identified weaknesses. We [redacted]
- [redacted]

[redacted]

- [redacted]
- [redacted] ~~supports mission processes in the areas of~~ [redacted] ~~However, the Agency has yet to fully address all of the weaknesses it found.~~ [redacted]
- [redacted]

[redacted]

- [redacted]

- [redacted]

[redacted] [redacted]

[redacted]

[redacted] [redacted]

- [redacted]

OMB Privacy Document Updates To Secure HVAs

OMB has established requirements for protecting and handling private or sensitive information in HVAs.[14] To ensure compliance with those requirements and to manage privacy risks, the Senior Agency Official for Privacy (SAOP) is required to identify the agency's HVAs that create, collect, use, process, store, maintain, disseminate, disclose, or dispose PII.

For each HVA identified, the SAOP shall ensure that all required privacy documentation and materials are complete, accurate, and up-to-date and that

[14] OMB M-19-03.

the Agency has a reliable process for identifying and assessing on an ongoing basis any changes to HVAs that may impact privacy or result in the need for additional or modified privacy documentation. This includes ensuring the Privacy Threshold Analyses and, if applicable, Privacy Impact Assessments are current and accurately reflect the information created, collected, used, processed, stored, maintained, disseminated, disclosed, or disposed of by the associated HVA information system.

However, the SAOP was not ensuring OMB requirements were met. For example, for [redacted] HVAs we assessed—[redacted]—the SAOP did not ensure the Privacy Threshold Analyses or applicable Privacy Impact Assessments are current and accurately reflect the information created, collected, used, processed, stored, maintained, disseminated, disclosed, or disposed of by the HVA.

DOT Has Not Properly Tested Its HVA Contingency and Incident Handling Activities

According to the National Institute of Standards and Technology (NIST),[15] an organization's IT plans need to be maintained to sustain the ability to prepare for, respond to, manage, and recover from disasters affecting the mission. NIST recommends using Test, Training, & Exercise events to test IT systems, train personnel, and exercise IT contingency and incident response plans. DOT requires all OAs to develop contingency plans for their information systems and coordinate contingency planning activities with incident-handling activities. Contingency planning addresses both information system restoration and implementation of alternative mission- or business-related processes when systems are compromised.

According to DHS,[16] departmental and agency headquarters continuity personnel and those entities that support organizational MEFs or PMEFs are required to participate in annual continuity exercises. Such exercises are part of an effective risk management program, the key to which is understanding potential risks and the organization's relation to those risks. Organizations can conduct risk

[15] NIST SP 800-84, *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities*, September 2006.

[16] DHS, *Federal Emergency Management Agency Federal Continuity Directive 1*, January 17, 2017.

assessments of their MEFs by completing a Business Impact Analysis for all threats and hazards. These organizations use this analysis to determine the mission and business processes and recovery criticality, along with outage and estimated maximum tolerable downtime for an information system. According to OMB, an information system with a maximum tolerable downtime of 12 hours or less can be designated as an HVA. Continuity plans also require a process for attaining capabilities at alternate locations as soon as possible but no later than 12 hours following the activation of the continuity plan for departments or agencies with MEFs and must be continuously performed for those entities with PMEFs.

Based on our review, DOT has not ensured that the contingency planning and incident handling activities for [redacted] HVAs we assessed are sufficient to respond to incidents because their maximum tolerable downtime exceeds the required 12 hours or less recovery timing goal for an HVA. The [redacted] HVAs that are not in compliance with the required maximum tolerable downtime goal are: [redacted] We were unable to obtain the actual maximum tolerable downtime data for [redacted].

Table 3. DOT HVAs Actual Maximum Tolerable Downtime (MTD) Relative to CISA Standard of 0–12 Hours

HVA System	OA	Actual MTD
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

Source: OIG analysis of HVA Systems Business Impact Analysis

We asked OA officials if they knew about the 0–12 hours maximum tolerable downtime goal for HVAs supporting any of DOT's PMEFs. They explained that those HVAs have not been given special consideration beyond the FISMA requirement for contingency planning and recovery timing goals based on system categorization.

The lack of a process for properly planning, testing, and implementing HVA contingency and incident-handling activities means that [redacted] The continuous performance of the HVAs is critical for ensuring DOT's resilience during a continuity event. The loss or corruption of HVAs coul [redacted]

Conclusion

Since 2015, Federal agencies have been required to focus on the protection of the Government's most critical and high-impact information and information systems. DOT's lack of an established organization-wide HVA governance program leaves the Department without the ability to take a strategic, enterprise-wide view of cyber risk and perform its PMEFs. Some DOT modes may not fully understand their critical system architecture and the impact a cyber-incident might have on their HVAs. Moreover, persistent delays in efforts to mitigate vulnerabilities in its HVAs raises questions about whether the Department has adequate cybersecurity protections in place. Finally, until DOT adequately tests its HVA contingency and incident-handling activities, it will not know whether its system assets can be considered "trusted information systems" that are capable of operating within defined levels of risk when faced with environmental disruptions, human errors, structural failures, or purposeful attacks.

Recommendations

To strengthen the cybersecurity of DOT's High Value Asset (HVA) Program, we recommend that the Department's Chief Information Officer:

1. Establish an effective HVA governance program based on the Office of Management and Budget's (OMB) Memorandum M-19-03 and the Department of Homeland Security's (DHS) Binding Operational Directive 18-02.
2. Review the [redacted] DOT HVAs listed on the Homeland Security Information Network at the time of our review and determine if any new HVAs should

be added, remove assets that are no longer HVAs, and confirm that HVAs are properly listed. At a minimum, the review should:

   a. Identify and prioritize its HVAs based on informational value, mission-essential function, and/or critical function to the Federal civilian enterprise.

   b. Consider the interconnectivity and dependencies of its systems when determining which ones should be HVAs.

   c. Develop a methodology for prioritizing HVAs based on criticality and mission importance.

3. Develop and implement an assessment approach for the Department's HVAs based on prioritization based on OMB Memorandum M-19-03 and DHS Binding Operational Directive 18-02.

4. Require the Senior Accountable Official for Risk Management for the [redacted] to report the Agency's plans for mitigating the remaining major or critical weaknesses to DHS every 30 days or another agreed-upon timeframe until all assessed findings are fully remediated.

5. Require the Senior Accountable Official for Risk Management for the [redacted] to report the Agency's plans for mitigating the remaining major or critical weaknesses every 30 days or another agreed-upon timeframe until all assessed findings are fully remediated.

6. Require DOT's Senior Agency Officials for Privacy to review the Department's HVAs and identify those that create, collect, use, process, store, maintain, disseminate, disclose, or dispose personally identifiable information; verify all required privacy documentation and materials are complete, accurate, and up to date; and provide confirmation upon completion.

7. Update and test the contingency plans for the Department's HVAs and confirm whether they can be recovered within a maximum tolerable downtime of 12 hours or less.

Agency Comments and OIG Response

We provided DOT with our draft report on September 1, 2023, and received its formal response on September 28, 2023. DOT's response is included in its entirety as an appendix to this report. DOT fully concurred with recommendations 1, 2, 3, 6, and 7 and provided appropriate planned actions and completion dates. DOT did not concur and requested we close recommendations 4 and 5.

We ask that the Department reconsider its position for recommendations 4 and 5 and its request for closure upon issuance of the final report. According to DOT's response, the Agency did not concur with recommendations 4 and 5 on two bases: (1) per OMB Memorandum M-17-25, Reporting Guidance for Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, the Senior Accountable Official for Risk Management is an agency-level responsibility and at DOT this responsibility is delegated to the DOT CIO, not officials within the Operating Administration; and (2) the Department of Homeland Security (DHS) confirmed OIG's findings have been remediated. While we do not take issue with the Department delegating Senior Accountable Official for Risk Management responsibility to the DOT CIO, officials within the Operating Administration were responsible at the time of our review, which was the basis for our recommendations. We acknowledge that the Department provided us with an e-mail from DHS HVA Program Management Office stating its records indicate that there were no reportable risks during the 2019 DHS assessment of [redacted]. We request that the Department provide us with a copy of the 2019 DHS assessment of [redacted] so we can verify whether our findings have been remediated.

We have updated our final report to reflect that [redacted]

Actions Required

We consider recommendations 1, 2, 3, 6 and 7 resolved but open pending completion of planned actions. We request that DOT reconsider its position and provide documentation to support closing recommendations 4 and 5. In accordance with DOT Order 8000.1C, we request that DOT provide its revised response within 30 days of the date of this report.

Exhibit A. Scope and Methodology

This performance audit was conducted between September 2021 and September 2023. We conducted this audit in accordance with generally accepted Government auditing standards. Those 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 objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. Our audit objectives for this self-initiated audit were to evaluate whether DOT (1) established an organization-wide HVA governance program to identify and prioritize HVAs and (2) assesses HVA security controls and ensures timely remediation of identified vulnerabilities.

To evaluate whether DOT established an organization-wide HVA governance program to identify and prioritize its HVAs, we performed a cybersecurity review of DOT's [redacted] HVAs systems. We determined whether DOT was meeting the requirements for OMB M-19-03, which defines agency requirements for strengthening the cybersecurity of Federal Agencies by enhancing the HVA Program. We interviewed DOT officials responsible for the governance of the Department's HVA program, as well as DOT officials responsible for overseeing the [redacted] HVAs. We collected and analyzed relevant data pertaining to DOT's internal controls for identifying and prioritizing HVAs, and reviewed DOT's methodology for prioritizing HVAs based on criticality and mission importance. Additionally, we met with DHS HVA officials to gain an understanding of its role in the Federal HVA program. Moreover, we determined whether DOT HVA systems were meeting the requirements for Presidential Policy Directive 40 - National Continuity Policy and its supporting Federal Continuity Directives 1, which directs agencies to incorporate continuity requirements to ensure continuation of DOT's Primary Mission Essential Functions and its OA's Mission Essential Functions.

To evaluate whether DOT assesses its HVAs security controls and ensures timely remediation of identified vulnerabilities, we determined whether DOT was meeting the requirements for DHS Binding Operational Directive 18-02, which defines agency requirements for ensuring effective identification and timely remediation of major and critical weaknesses to HVA systems based on DHS HVA assessments. We interviewed DOT officials responsible for coordinating DOT's participation in DHS-led assessments, as well DOT officials responsible for reporting the security status of the DOT's HVAs to DHS. We reviewed DHS-led assessment reports on DOT HVA systems, which include Risk and Vulnerability Assessments, and Security Architecture Reviews. We reviewed DHS recommendations of DOT HVA systems and determined if corrective actions were taken. We also met with the DHS HVA officials to gain an understanding of the HVA reporting requirements for Federal agencies. We also determined whether DOT was meeting FISMA requirements for the HVA systems as the department reported it relies on its internal FISMA reviews to assess security weakness. We reviewed security authorization documentation provided for DOT's HVAs, including but not limited to system categorization documentation, contingency plans, system security plans, security assessment reports, Plans of Action and Milestone data, and Executive Summaries. We provided the results of our assessment of the FISMA documentation to DOT HVA security officials for review and considered their comments when applicable.

Exhibit B. Organizations Visited or Contacted

Federal Aviation Administration

Federal Highway Administration

Federal Motor Carrier Safety Administration

Federal Railroad Administration

Federal Transit Administration

Great Lakes St. Lawrence Seaway Development

Maritime Administration

National Highway Traffic Safety Administration

Office of the Chief Information Officer

Office of Inspector General

Office of the Secretary of Transportation

Pipeline and Hazardous Materials Safety Administration

Other Organizations

Department of Homeland Security

Exhibit C. List of Acronyms

ARTEMIS	Advanced Retrieval Tire, Equipment, Motor Vehicle Information System
ASR-11	Airport Surveillance Radar Model 11
AVSR	Aviation Registry Application
BOD	Binding Operational Directives
CAMS	Comprehensive Academic Management System
CASTLE	Consolidated Automated System for Time and Labor Entry
CE	Cloud Environment
CISA	Cybersecurity and Infrastructure Security Agency
CISO	Chief Information Security Officer
COE	Common Operating Environment
CSAM	Cybersecurity Assessment and Management
CUI	Controlled Unclassified Information
DHS	Department of Homeland Security
DOT	Department of Transportation
FAA	Federal Aviation Administration
FCD	Federal Continuity Directive
FCEE	Federal Civilian Enterprise Essential
FHWA	Federal Highway Administration
FISMA	Federal Information Security Modernization Act
FMCSA	Federal Motor Carrier Safety Administration
FMS	Financial Management System
FOIA	Freedom of Information Act
FRA	Federal Railroad Administration
FTA	Federal Transit Administration
FTI	FAA Telecommunications Infrastructure

GAGAS	Generally Accepted Government Auditing Standards
GLS	Great Lakes St. Lawrence Seaway Development
GMSS	Grants Management Solutions Suite
GTS	Grants Tracking System
HVA	High Value Assets
IT	Information Technology
ITS	Investigative Tracking System
LAN	Local Area Network
LCO	Lock Control and Operation
MARAD	Maritime Administration
MEF	Mission-Essential Function
NAS	National Airspace System
NDP	NAS Defense Program
NESG	NAS Enterprise Security Gateway
NHTSA	National Highway Traffic Safety Administration
NIST	National Institute of Standards and Technology
NPMS	National Pipeline Mapping System
NSTRC	National Sobriety Testing Resource Center
OA	Operating Administrations
OCIO	Office of the Chief Information Officer
OIG	Office of Inspector General
OMB	Office of Management and Budget
OST	Office of the Secretary of Transportation
PHMSA	Pipeline and Hazardous Materials Safety Administration
PII	Personally Identifiable Information
POC	Points of Contact
PMEF	Primary Mission-Essential Function
PPD	Presidential Policy Directive
PSES	Personnel Security Enterprise System

SAOP	Senior Agency Official for Privacy
SBSS	Surveillance and Broadcast Service System
USMMA	US Merchant Marine Academy
VSCS	Voice Switching and Control System
WS	Web System

Exhibit D. Major Contributors to This Report

LEON **LUCAS**	PROGRAM DIRECTOR
JO'SHENA **JAMISON**	SENIOR IT SPECIALIST
JENELLE **MORRIS**	SENIOR IT SPECIALIST
ANTIONE **SEARCY**	SENIOR IT SPECIALIST
JANE **LUSAKA**	SUPERVISORY WRITER-EDITOR
SUSAN **CROOK-WILSON**	SUPERVISORY WRITER-EDITOR
SEETHA **SRINIVASAN**	SENIOR COUNSEL

Appendix. Agency Comments

Memorandum

U.S. Department of Transportation
Office of the Secretary of Transportation

Subject: **INFORMATION:** Management Response to the Office of the Inspector General (OIG) Draft Report on High-Value Assets (HVA) Program

From: Jay Ribeiro
Associate Chief Information Officer /
Chief Information Security Officer
Office of the Chief Information Officer

LICERIO GAMBOA RIBEIRO JR
Digitally signed by LICERIO GAMBOA RIBEIRO JR
Date: 2023.09.28 18:08:44 -04'00'

To: Kevin Dorsey
Assistant Inspector General for
Information Technology Audits

The U.S. Department of Transportation (DOT or Department) is committed to enhancing and fortifying its Information Security Program. The Department's Chief Information Officer (CIO) continues to prioritize cybersecurity as the top priority of the Office of the Chief Information Officer (OCIO), consistently elevating its importance across the Department. This steadfast commitment from high-level executives has allowed DOT to make continuous progress on various fronts, in harmony with the directives set forth in Executive Order (EO) 14028. As part of this aggressive and critical project, the OCIO welcomed a new Director of FISMA and High-Value Asset (HVA) Compliance in March 2023, whose primary role is to reduce the number of outstanding FISMA recommendations and revamp the Department's HVA program. This initiative begins with the establishment of a dedicated office responsible for overseeing the program throughout the agency.

In reviewing the OIG draft report, we identified a significant inaccuracy regarding [redacted]. The OIG report states, "[redacted]" This statement is not correct. The [redacted] was assessed by the [redacted] in September 2021, April 2022, and April 2023.

Based on our review of the draft report, we concur, as written, with recommendations 1, 2, 3, 6, and 7 to strengthen the cybersecurity of DOT's HVA program and plan to implement these recommendations during our FY24 HVA Program Transformation project by August 31, 2024. We do not concur with recommendations 4 and 5 on two bases: (1) per OMB Memorandum M-17-25, Reporting Guidance for Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, the Senior Accountable Official for Risk Management is an agency-level responsibility and at DOT this responsibility is delegated to the DOT CIO, not officials within the Operating Administrations; and (2) the Department of Homeland Security (DHS) confirmed the OIG cited findings have been remediated.

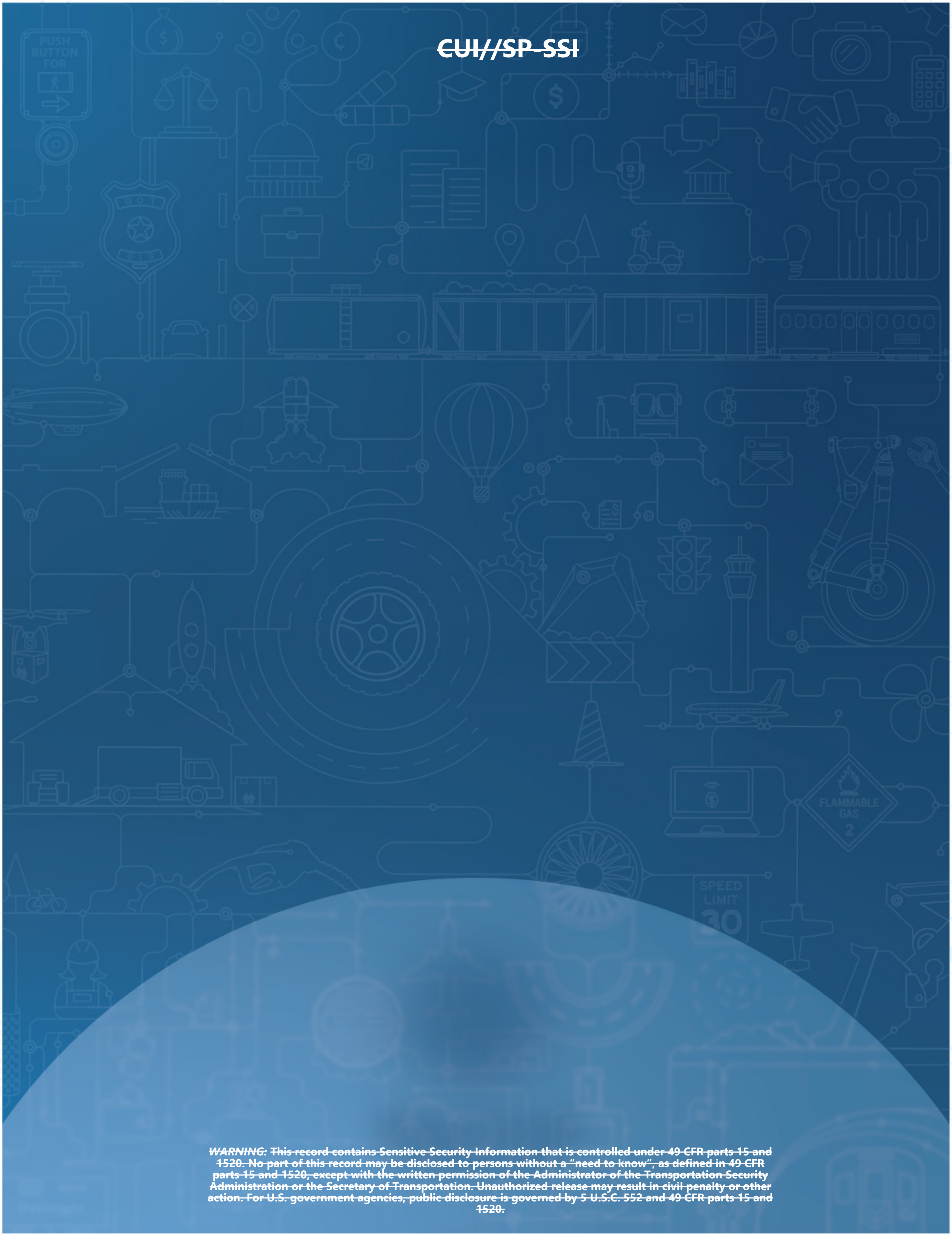
Additional Comments on Non-Concurs:

Recommendation 4: Require the Senior Accountable Official for Risk Management for the [redacted] to report the Agency's plans for mitigating the remaining major or critical weaknesses to DHS every 30 days or another agreed-upon timeframe until all assessed findings are fully remediated.

Response: *The DOT CIO has ensured that the* [redacted] *remediated all major and critical weaknesses identified by DHS. The DOT CIO received confirmation from DHS in September 2021 that the finding was remedied. In September 2023, DHS reconfirmed that no new risks were found during the 2019 HVA Assessment. This evidence was shared with OIG on September 26, 2023. We request OIG close this recommendation within 30 days of OIG's final report.*

Recommendation 5: Require the Senior Accountable Official for Risk Management for the [redacted] to report the Agency's plans for mitigating the remaining major or critical weaknesses every 30 days or another agreed-upon timeframe until all assessed findings are fully remediated.

Response: *During the audit, OIG received information demonstrating that all cited weaknesses have been addressed; however, the OIG draft report only states "DHS assessed* [redacted] *twice. In September 2016, DHS completed a risk and vulnerability assessment… and made five recommendations. In February 2017, DHS released a draft security architecture review of* [redacted] *and made two recommendations to* [redacted]*." The DOT CIO has received confirmation from DHS that all recommendations were remediated, and no new findings were found during the 2019 HVA Assessment. This evidence was shared with OIG on September 26, 2023. We request OIG close this recommendation within 30 days of OIG's final report.*



~~*WARNING*: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.~~