



U.S. DEPARTMENT OF HOMELAND SECURITY **OFFICE OF INSPECTOR GENERAL**

OIG-25-08

January 15, 2025

FINAL REPORT

Cybersecurity System Review of a Selected High Value Asset at CISA





OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

Washington, DC 20528 | www.oig.dhs.gov

January 15, 2025

MEMORANDUM FOR: Robert Costello
Chief Information Officer
Cybersecurity and Infrastructure Security Agency

FROM: Joseph V. Cuffari, Ph.D.
Inspector General

SUBJECT: *Cybersecurity System Review of a Selected High Value Asset at CISA*

**JOSEPH V
CUFFARI** Digitally signed by
JOSEPH V CUFFARI
Date: 2025.01.13
15:42:21 -05'00'

Attached for your action is our final report, *Cybersecurity System Review of a Selected High Value Asset at CISA*. We incorporated the formal comments provided by your office.

The report contains one recommendation aimed at CISA's assessment process to better secure Federal agencies' Tier 1 HVA systems. Your office concurred with the one recommendation. Based on information provided in your response to the draft report, we consider the recommendation open and resolved. Once your office has fully implemented the recommendation, please submit a formal closeout letter to us within 30 days so that we may close the recommendation. The memorandum should be accompanied by evidence of completion of agreed-upon corrective actions and of the disposition of any monetary amounts.

Please send your response or closure request to oigauditsfollowup@oig.dhs.gov.

Consistent with our responsibility under the *Inspector General Act*, we will provide copies of our report to congressional committees with oversight and appropriation responsibility over the Department of Homeland Security. We will post the report on our website for public dissemination.

Please contact me with any questions, or your staff may contact Kristen Bernard, Deputy Inspector General for Audits, at (202) 981-6000.

Attachment



DHS OIG HIGHLIGHTS

Cybersecurity System Review of a Selected High Value Asset at CISA

January 15, 2025

Why We Did This Review

The Federal Government requires agencies to protect HVAs against evolving cyber threats. We conducted this review to determine whether CISA has implemented effective technical controls to protect sensitive information on a selected HVA system.

What We Recommend

We made one recommendation to improve CISA's assessment process to better secure Federal agencies' Tier 1 HVA systems.

For Further Information:

Contact our Office of Public Affairs at (202) 981-6000, or email us at:

DHS-OIG.OfficePublicAffairs@oig.dhs.gov.

What We Found

The Cybersecurity and Infrastructure Security Agency (CISA) did not implement effective controls for the selected High Value Asset (HVA) system per Federal and departmental requirements. CISA developed policies and procedures to reduce risks to sensitive information stored on the selected HVA system. However, we identified security deficiencies in two of eight security and privacy controls required by the National Institute of Standards and Technology pertaining to:

- access controls; and
- awareness and training.

These deficiencies occurred because CISA did not have effective continuous monitoring of the selected HVA system. Without effective controls, CISA could not be assured that sensitive information stored and processed by the selected HVA system was protected and secured.

As part of this review, we also identified inconsistencies in CISA's Tier 1 HVA Assessment Report of the selected HVA system, dated March 2023. These issues are indicators that CISA's HVA assessment process did not identify all security risks put forth in CISA's security alerts.

CISA Response

CISA concurred with our recommendation. We included a copy of CISA's comments in Appendix B.



OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

Table of Contents

Background	1
Results of Review	2
CISA Developed Policies and Procedures to Reduce Risks to Sensitive Information Stored on a Selected System.....	3
CISA Did Not Implement All Security and Privacy Controls to Protect Sensitive Information Stored on a Selected HVA System	3
CISA Can Improve Its Tier 1 HVA System Assessment Process.....	7
Recommendation	9
CISA Comments and OIG Analysis	9
Appendix A: Objective, Scope, and Methodology.....	10
DHS OIG’s Access to DHS Information.....	11
Appendix B: CISA Comments on the Draft Report	12
Appendix C: Office of Audits Major Contributors to This Report.....	15
Appendix D: Report Distribution	16

Abbreviations

CISA	Cybersecurity and Infrastructure Security Agency
FISMA	<i>Federal Information Security Modernization Act</i>
HVA	High Value Asset
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
SBU	Sensitive but Unclassified
SP	Special Publication



Background

The United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public and private sectors, as well as the security and privacy of all Americans. The Federal Government has seen numerous information security incidents affecting the integrity, confidentiality, and/or availability of Government information, systems, and services. The Department of Homeland Security Office of Inspector General and the U.S. Government Accountability Office have both identified preventing cyberattacks as a major management and performance challenge.¹

In 2015, the Office of Management and Budget (OMB) created the High Value Asset (HVA) initiative, which required Federal agencies to identify their most critical assets.² The Federal Government requires agencies to protect HVAs against evolving cyber threats. Per OMB Memorandum-19-03, *Strengthening the Cybersecurity of Federal Agencies by Enhancing the High Value Asset Program*, agencies may designate Federal information or a Federal information system as an HVA when it relates to one or more of the following categories: informational value, mission essential, or Federal Civilian Enterprise Essential. In addition, the President directed the Federal Government to improve its efforts to identify, deter, protect against, detect, and respond to these actions and actors.³

Established by the *Cybersecurity and Infrastructure Security Agency Act of 2018*, the Cybersecurity and Infrastructure Security Agency (CISA) serves as America's cyber defense agency and as the national coordinator for critical infrastructure security and resilience. CISA categorizes HVA systems into Tier 1 and non-Tier 1. Tier 1 denotes HVA systems of critical impact to both the agency and our Nation; non-Tier 1 denotes HVA systems of significant impact to both the agency and our Nation.

The National Institute of Standards and Technology (NIST) established controls for systems and organizations. The use of these controls is mandatory for Federal information systems. For instance, NIST Special Publication (SP) 800-53, Revision 5,⁴ sets forth information security standards and guidelines, including minimum requirements for Federal information systems. NIST also provides agencies with a common structure to identify and manage cybersecurity risks across the enterprise, in alignment with five functions from its Cybersecurity Framework (Identify, Protect, Detect, Respond, Recover).⁵

¹ [Department of Homeland Security's Annual Performance Report \(APR\) for FY 2021–2023](#).

² OMB M-16-03, [Fiscal Year 2015–2016 Guidance on Federal Information Security and Privacy Management Requirements](#), October 30, 2015.

³ Executive Order 14028, [Executive Order on Improving the Nation's Cybersecurity](#), May 12, 2021.

⁴ NIST SP 800-53, Revision 5, [Security and Privacy Controls for Information Systems and Organizations](#), September 2020.

⁵ [Framework for Improving Critical Infrastructure Cybersecurity](#), Version 1.1, April 16, 2018.



OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

We conducted this review as part of our *Federal Information Security Modernization Act of 2014* (FISMA)⁶ oversight to determine whether CISA implemented effective technical controls to protect sensitive information on a selected HVA system. We judgmentally selected one HVA (hereafter referred to as “the selected HVA system”) for this review. The selected HVA system is an online portal that housed information that one of the critical infrastructure sectors submits to CISA. As of January 2024, CISA designated the system as a Tier 1 HVA, with an overall security categorization as “Moderate,” including “Moderate” for all three security objectives (Confidentiality, Integrity, and Availability). This report is one from a series of reviews on the Department’s HVAs. We plan to incorporate the results from this review into our fiscal year 2024 FISMA submission.

On January 26, 2024, DHS personnel received credible information of a potential compromise to the selected HVA environment. CISA immediately initiated incident response procedures, including isolating the selected HVA system from the DHS network. CISA’s Office of the Chief Information Officer notified us about the incident on January 31, 2024. Because the selected HVA system was removed from the network, we did not perform technical testing during our review.

On March 25, 2024, DHS determined that this incident met the definition of a “major incident” as defined in OMB M-24-04⁷ and subsequently notified Congress of the incident on March 29, 2024. The DHS Network Operations and Security Center determined in a March 25, 2024, incident report that the selected HVA system will remain offline and will not be re-constituted.

We reviewed actions taken by the selected HVA system’s personnel over the last 3 years to address previous CISA alerts related to the compromised commercial product. We determined the selected HVA system’s personnel took the appropriate actions to address the CISA alerts per the guidance provided by CISA and the product manufacturer. Because CISA does not plan to bring the system online again, we are not making any recommendations to correct the deficiencies we identified related to NIST SP 800-53 controls.

Results of Review

CISA did not implement effective technical controls for the selected HVA system per Federal and departmental requirements. CISA developed policies and procedures to reduce risks to sensitive information stored on the selected HVA system. However, we identified security deficiencies in two of eight security and privacy controls required by NIST pertaining to:

- access controls; and

⁶ [Federal Information Security Modernization Act of 2014](#), Public Law 113-283, December 18, 2014.

⁷ OMB M-24-04, [Fiscal Year 2024 Guidance on Federal Information Security and Privacy Management Requirements](#), December 4, 2023.



- awareness and training.

These deficiencies occurred because CISA did not have effective continuous monitoring of the selected HVA system. Without effective controls, CISA could not be assured that sensitive information stored and processed by the selected HVA system was protected and secured.

As part of this review, we also identified inconsistencies in CISA's Tier 1 HVA Assessment Report of the selected HVA system, dated March 2023. These issues are indicators that CISA's HVA assessment process did not identify all security risks put forth in CISA's security alerts.

CISA Developed Policies and Procedures to Reduce Risks to Sensitive Information Stored on a Selected System

NIST⁸ requires agencies to develop a plan for managing supply chain risks associated with the research and development, design, manufacturing, acquisition, delivery, integration, operations and maintenance, and disposal of systems, system components, or system services. Based on our review of documentation provided by CISA officials, we determined CISA had developed policies and procedures to help protect sensitive information stored on the selected HVA system. For example, CISA had:

- developed a system-specific supply chain risk management policy; and
- established policies and procedures requiring audit trails be generated for the selected HVA system.

CISA Did Not Implement All Security and Privacy Controls to Protect Sensitive Information Stored on a Selected HVA System

CISA did not implement effective controls for the selected HVA system per Federal and departmental requirements. Specifically, CISA did not effectively implement the required security and privacy controls⁹ to protect the sensitive information stored and processed by the selected HVA system in two of eight NIST SP 800-53 control families tested. Table 1 shows the deficiencies we identified through control family testing and the corresponding function in the NIST Cybersecurity Framework.

⁸ NIST SP 800-53, Revision 5, [Security and Privacy Controls for Information Systems and Organizations](#), September 2020.

⁹ According to NIST [SP 800-53, Revision 5](#), there are 20 control families. Our review focused on 8 of 20 control families listed in NIST SP 800-53, Revision 5.



OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

Table 1. Deficiencies Identified in NIST SP 800-53 Control Families Tested and Corresponding Functions in the NIST Cybersecurity Framework

NIST SP 800-53		NIST Cybersecurity Framework	
Control Family Tested	Deficiencies Identified	Function	FISMA Domain
Risk Assessment	No	Identify	Risk Management
Supply Chain Risk Management	No		Supply Chain Risk Management
Configuration Management	No	Protect	Configuration Management
Access Control	Yes		Identity and Access Management
Audit and Accountability	No		Data Protection and Privacy
Awareness and Training	Yes		Security Training
Assessment, Authorization, and Monitoring	No	Detect	Information Security Continuous Monitoring
Incident Response	No	Respond	Incident Response

Source: Compiled by DHS OIG based on NIST SP 800-53, Revision 5, NIST Cybersecurity Framework, and Fiscal Year 2024 FISMA reporting metrics.



Control Family – Access Control

CISA Did Not Always Ensure that Inactive User Accounts Were Removed or Disabled

NIST¹⁰ requires agencies to disable expired and inactive accounts. Agencies must:

- identify system users with administrative privileges and provide additional scrutiny by organizational personnel responsible for approving such accounts;
- document accounts that are allowed or prohibited for use within a system; and
- define or specify the authorized users of the system, group and role membership, and access authorizations (i.e., privileges) for each account.

CISA required the selected HVA system to automatically disable accounts of DHS Federal and contractor users after a 45-day period. In addition, the Information System Owner and Information System Security Officer should have performed an annual review of the users who had signed a Privileged User’s Rules of Behavior and validated the need for privileged users to retain their elevated privileges.

CISA did not always promptly remove inactive users from the selected HVA system. In January 2024, we received three active user lists with a total of 7,279 users, which included a mix of Sensitive but Unclassified (SBU) (onsite/administrators), Federal, and Industry users. Based on the policies and procedures obtained, CISA defined the Federal and Industry users as required. CISA did not provide us with any written documentation that defines the SBU users. According to CISA personnel, Congress decided to stop providing funding for the selected HVA system in July 2023. As a result, although Industry users were included in the active user lists, they could not log on to the selected HVA system. Therefore, we excluded the 4,503 Industry users from our access control analysis.

Of the 2,776 remaining SBU and Federal users, we determined that 1,124 (40 percent) had not logged onto the system for an extended time but still had active accounts, contrary to NIST and CISA’s internal policy. For example,

- 24 (12 from each group) user accounts had not logged on since their accounts were created.
- Eight user accounts had not logged on for over 12 months (since January 2023). Two of these eight user accounts had not logged on since April 2021.

¹⁰ NIST SP 800-53, Revision 5, [Security and Privacy Controls for Information Systems and Organizations](#), September 2020.



Inactive accounts that are not removed or disabled create a significant cybersecurity risk to the system due to the possibility of malicious actors obtaining access to valuable resources.

Control Family – Awareness and Training

CISA Did Not Ensure All HVA System Users Received Required Security Awareness Training

FISMA¹¹ directs agencies to provide security awareness training to personnel, including contractors and other users of information systems that support the operations and assets of the agency. OMB¹² requires agencies to implement mandatory agency-wide information security and privacy awareness training programs. NIST¹³ instructs agencies to provide initial security and privacy literacy training to system users and thereafter to provide refresher training at an agency-defined frequency. DHS¹⁴ requires that all users accessing DHS systems receive initial and annual basic cybersecurity awareness training. Finally, CISA requires its users to complete cybersecurity awareness training at least annually. We found CISA did not ensure all HVA system users received the required security awareness training.

To ensure system users received the required security awareness training, we requested training records for all 19 SBU users and a judgmental sample of 20 Federal users and 30 Industry users within the last 18 months. According to CISA personnel, CISA could not provide training records for the Industry users because the system was removed from the DHS network and CISA stored Industry users' training records on that system. Based on the information CISA provided, we determined that 6 of 39 (15 percent) of the SBU and Federal users sampled did not receive the required security awareness training during the period. Specifically, of those six:

- One did not take initial cybersecurity awareness training until after we requested records.
- One did not take annual cybersecurity awareness training for the past 2 years.
- Two did not take initial or annual cybersecurity awareness training and were listed as “CISA contractors” with “wrong email addresses provided.”
- Two did not take initial or annual cybersecurity awareness training and were listed as “no longer in CISA” and “no training records within the last 18 months.”

The deficiencies we identified occurred because CISA did not have effective continuous monitoring for the selected HVA system. Without effective controls, CISA could not be assured that sensitive information stored and processed by the selected HVA system was protected and

¹¹ [Federal Information Security Modernization Act of 2014](#), Public Law 113-283, December 18, 2014.

¹² OMB Circular A-130, [Managing Information as a Strategic Resource](#), Revised July 2016.

¹³ NIST SP 800-53, Revision 5, [Security and Privacy Controls for Information Systems and Organizations](#), September 2020.

¹⁴ DHS Policy Directive 4300A, v13.3, [Information Technology System Security Program, Sensitive Systems](#), February 13, 2023.



secured. In addition, the authorizing official could not make credible, risk-based decisions about the system. Because of these deficiencies, CISA was less equipped to protect the selected HVA system and could not ensure it would be able to quickly detect, respond to, and recover from a cyberattack.

CISA Can Improve Its Tier 1 HVA System Assessment Process

OMB¹⁵ requires DHS, a third-party assessor, or an agency's independent assessment entity to perform HVA assessments and incorporate the HVA assessments as part of existing agency cybersecurity programs. As part of its cybersecurity responsibilities, CISA¹⁶ requires selected HVA systems across the Federal Government to participate in DHS-led HVA assessments, ensure timely remediation of identified vulnerabilities, and report mitigation plans and progress. Further, CISA has issued alerts and other publications advising Federal agencies and private sector partners to remove or disable inactive accounts. Below are examples of recent CISA alerts:

- *Weak Security Controls and Practices Routinely Exploited for Initial Access* (Alert Code AA22-137A, December 8, 2022) recommends ensuring there are processes in place for the entry, exit, and internal movement of employees. In addition, it recommends the deletion of unused accounts, and immediate removal of access to data and systems from accounts of exiting employees who no longer require access. This included the deactivation of service accounts, and activation only when maintenance is performed.
- *Advanced Persistent Threat Activity Exploiting Managed Service Providers* (Alert Code TA18-276B, June 30, 2020) recommends the establishment of policies and procedures for the prompt removal of unnecessary accounts and groups from the enterprise. Additionally, organizations should implement a robust and continuous user management process to ensure accounts of offboarded employees are removed.

Though CISA performed an HVA assessment on the system in March 2023, we found indicators that suggest the HVA assessment process may not be effective to address security risks that arise from not disabling or removing inactive accounts as recommended in the aforementioned CISA security alerts.

According to CISA's March 2023 HVA Assessment Report, the selected HVA system has a security environment that excels in meeting compliance requirements. All observations and recommendations from this HVA assessment are based on Federal guidance or leading practices and reflect CISA subject matter experts' consensus opinion. The report focuses on providing

¹⁵ OMB M-19-03, [Strengthening the Cybersecurity of Federal Agencies by enhancing the High Value Asset Program](#), December 10, 2018.

¹⁶ CISA Binding Operational Directive 18-02, [Securing High Value Assets](#), May 7, 2018.



OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

agency executive leadership with a professional review of the HVA's security architecture with emphasis on identifying the technical gaps and their associated cybersecurity risks.

CISA's HVA assessment process can be improved, based on the deficiencies we identified in the Access Control family. These deficiencies include inactive accounts that were not disabled per CISA's 45-day requirement. According to NIST SP 800-53, Revision 5, the requirement for disabling and removing accounts is part of the Account Management control within the Access Control family. The CISA HVA program office's HVA assessment did not identify 24 user accounts that had not logged on since their creation. Two of these users had not logged on since April 2021 and should have been identified during the March 2023 assessment. The HVA assessment also included an HVA Control Overlay¹⁷ that marked the security controls for Access Control as implemented, but then flagged the Automated Temporary and Emergency Account Management control as noncompliant.

Based on the deficiencies and the inactive accounts we identified in the Access Control family, we determined that CISA did not assess why some of the accounts were created but never logged onto, and why inactive accounts were not removed or disabled. CISA also did not always follow the best practices it included in its own security alerts to remove or disable inactive accounts.

Further, we found the following issues in the HVA program office assessment results:

- Although CISA identified 16 penetration testing scenarios in the March 2023 HVA Assessment Report, the assessor only listed the results for six scenarios in Table 11 of the HVA Assessment Report. Three of the six scenarios were listed as "not conducted." We could not determine whether the assessor performed the other 10 scenarios. Although the report refers readers to Appendix A for, "Detailed findings and recommended mitigations," we found Appendix A only listed CISA Authorities.
- Based on our review of the 14 tools CISA used to complete the HVA assessment, at least 2 of the 14 tools have the capabilities or features to identify inactive accounts, if CISA chose to perform the testing.

When questioned as to why CISA's HVA assessment team did not review inactive accounts as part of the HVA Control Overlay, or as recommended by CISA's security alerts, an HVA program official stated that CISA's Tier 1 assessments are not an audit. We asked to meet with the assessor who performed the 2023 assessment, but we were told the assessor had left CISA. When we asked whether CISA performed a supervisory review of the assessment results before they were

¹⁷ CISA uses the HVA Control Overlay in its HVA assessments to focus its analysis on the most critical cybersecurity controls applicable to HVAs. The HVA Control Overlay contained 18 security control families from NIST SP 800-53, Revision 5, including the Access Control family and the Awareness and Training family.



OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

released, we were told CISA does not retain internal comments made and only peer review comments would have been tracked. CISA told us it did not receive any peer review comments from program office staff.

The deficiencies we identified in CISA's HVA Assessment Report suggest CISA's HVA assessment process may not effectively protect sensitive information or identify all security risks put forth in CISA's security alerts. Until CISA revises its HVA assessment process, CISA cannot ensure its efforts are improving the security of the Tier 1 HVA systems that it assesses.

Recommendation

Recommendation 1: We recommend the CISA Director strengthen CISA's Tier 1 High Value Asset Assessment Process to include the major security threats that it identifies in its alerts and notifications to Federal agencies as part of the assessment.

CISA Comments and OIG Analysis

We obtained written comments on a draft of this report from CISA. We reviewed CISA's management comments, as well as the technical comments previously submitted and updated the report as appropriate. CISA concurred with the recommendation, which we consider open and resolved. In the comments, CISA indicated it appreciated our work on this review. CISA said it will conduct a comprehensive review of the HVA assessment process and determine appropriate action, as needed, to ensure alignment with broader CISA guidance to the Federal community. A summary of CISA's responses and our analysis follows.

CISA Comments to Recommendation 1: Concur. CISA's Cybersecurity Division will conduct a comprehensive review of the HVA assessment process and determine appropriate action, as needed, to ensure alignment with broader CISA guidance to the Federal community. This will include major security threats identified in CISA's alerts and notifications to Federal agencies. Estimated Completion Date: June 30, 2025.

OIG Analysis: CISA's actions are responsive to the recommendation, which will remain open and resolved until CISA provides documentation showing that all planned corrective actions are completed.



Appendix A: Objective, Scope, and Methodology

The Department of Homeland Security Office of Inspector General was established by the *Homeland Security Act of 2002* (Pub. L. No. 107–296) by amendment to the *Inspector General Act of 1978*.

Our objective was to determine whether CISA has implemented effective technical controls to protect sensitive information on a selected HVA system. We focused our review on one CISA HVA system. To accomplish our objective, we determined whether CISA had developed policies and procedures in the following areas:

- patch and configuration management
- supply chain risk management
- user account access management
- audit trails
- data privacy protection
- security awareness and role-based trainings
- incident response

We reviewed documentation and artifacts CISA provided for the selected HVA system to evaluate CISA’s implementation of selected NIST SP 800-53 Revision 5 controls.¹⁸ Additionally, we performed judgmental sampling in the areas of user account management, security awareness training, and role-based training. We also analyzed system user and privileged user lists CISA provided and reviewed information from the Department’s compliance management system.

When writing the report, we considered the potential for sensitivity issues under DHS Management Directive 11042.1, *Safeguarding Sensitive but Unclassified Information*, and generalized findings as appropriate to avoid disclosing information designated as sensitive by the Department.

We conducted this review between December 2023 and May 2024, under the authority of the *Inspector General Act of 1978*, as amended, 5 United States Code §§ 401-424, and according to the *Quality Standards for Inspection and Evaluation* issued by the Council of the Inspectors General on Integrity and Efficiency.

¹⁸ NIST SP 800-53, Revision 5, [Security and Privacy Controls for Information Systems and Organizations](#), September 2020.



OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

DHS OIG's Access to DHS Information

During this review, CISA provided timely responses to our requests for information and did not delay or deny access to information we requested.



OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

Appendix B: CISA Comments on the Draft Report

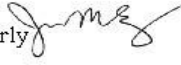


U.S. Department of Homeland Security
Cybersecurity & Infrastructure Security Agency
Office of the Director
Washington, DC 20528

BY ELECTRONIC SUBMISSION

October 28, 2024

MEMORANDUM FOR: Joseph V. Cuffari, Ph.D.
Inspector General

FROM: Jen Easterly 
Director
Cybersecurity and Infrastructure Security Agency

SUBJECT: Management Response to Draft Report: "Cybersecurity System Review of a Selected High Value Asset at CISA" (Project No. 24-009-AUD-CISA)

Thank you for the opportunity to comment on this draft report. The Cybersecurity and Infrastructure Security Agency (CISA) appreciates the work of the Office of Inspector General (OIG) in planning and conducting its review and issuing this report.

CISA leadership is pleased to acknowledge the OIG's positive recognition that, on January 26, 2024, following receipt of credible information of a potential compromise to the selected High Value Asset (HVA) environment, CISA immediately initiated incident response procedures, including the isolation of the selected CISA HVA system from the U.S. Department of Homeland Security network. CISA remains committed to strengthening the Tier 1¹ HVA assessment process to address major security threats identified in CISA's alerts and notifications to Federal agencies.

Regarding OIG's draft report identifying security control deficiencies pertaining to (1) access controls, and (2) awareness and training, it is important for the reader to understand that after evaluating the risk and mission conditions, CISA leadership made the immediate determination that the system should not come back online. Because the system is offline, any risks have been mitigated.

On September 26, 2024, CISA granted an Authority to Operate for the CISALearn system that will serve as the agency's enterprise learning platform. Upon implementation of CISALearn in fiscal year 2025, this innovative training platform will ensure that users have up-to-date cybersecurity awareness training and appropriate account access.

¹ Tier 1 denotes HVA systems of critical impact to both agency and the nation; non-Tier 1 denotes HVA systems of significant impact to both the agency and to the nation.



OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

Since October 2023, more than 30 CISA information technology systems have migrated to the CISA Net Identity Credential and Access Management solution, enhancing and modernizing system capabilities including onboarding, offboarding, account inactivity, privileged access, and reporting, while lowering overall enterprise risk. CISA's Office of the Chief Information Officer will continue to work diligently to strengthen the security of CISA's systems.

The draft report contained one recommendation with which CISA concurs. Attached find our detailed response to the recommendation. CISA previously submitted technical comments addressing several accuracy, contextual and other issues under a separate cover for OIG's consideration, as appropriate.

Again, thank you for the opportunity to review and comment on this draft report. Please feel free to contact me if you have any questions. We look forward to working with you again in the future.

Attachment



OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

Attachment: Management Response to Recommendation Contained in OIG 24-009-AUD-CISA

OIG recommended that the Director of CISA:

Recommendation 1: Strengthen CISA's Tier 1 High Value Asset Assessment Process to include the major security threats that it identifies in its alerts and notifications to Federal agencies as part of the assessment.

Response: Concur. CISA's Cybersecurity Division will conduct a comprehensive review of the HVA assessment process and determine appropriate action, as needed, to ensure alignment with broader CISA guidance to the federal community. This will include major security threats identified in CISA's alerts and notifications to Federal agencies. Estimated Completion Date: June 30, 2025.



Appendix C:
Office of Audits Major Contributors to This Report

Craig Adelman, Assistant Inspector General, IT Audits
Richard Harsche, Director, Disaster Management and Infrastructure Protection
Chiu-Tong Tsang, Director, Cybersecurity and Intelligence Division
Shawn Hatch, Audit Manager
Lawrence Polk, IT Cybersecurity Specialist
Sonya Griffin, Auditor-in-Charge
Garrick Greer, Auditor
Bridgette OgunMokun, Auditor
Omar Russell, Auditor
Lauren Barrick, Auditor
Aishia LaCount, Auditor
Eduvirgen Peralta-Cruz, Communications Analyst
Victor Leung, Referencer



Appendix D: Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy Chiefs of Staff
General Counsel
Executive Secretary
Director, GAO/OIG Liaison Office
Under Secretary, Office of Strategy, Policy, and Plans
Assistant Secretary for Office of Public Affairs
Assistant Secretary for Office of Legislative Affairs
Director, CISA
CIO, CISA
Audit Liaison, CISA

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees

Additional Information

To view this and any other DHS OIG reports, Please visit our website: www.oig.dhs.gov

For further information or questions, please contact the DHS OIG Office of Public Affairs via email: DHS-OIG.OfficePublicAffairs@oig.dhs.gov



DHS OIG Hotline

To report fraud, waste, abuse, or criminal misconduct involving U.S. Department of Homeland Security programs, personnel, and funds, please visit: www.oig.dhs.gov/hotline

If you cannot access our website, please contact the hotline by phone or mail:

Call: 1-800-323-8603

U.S. Mail:
Department of Homeland Security
Office of Inspector General, Mail Stop 0305
Attention: Hotline
245 Murray Drive SW
Washington, DC 20528-0305