U.S. DEPARTMENT OF HOMELAND SECURITY

OFFICE OF INSPECTOR GENERAL

OIG-25-43 September 23, 2025

FINAL REPORT

Inadequate Cybersecurity Rendered DHS Headquarters High-Value System Vulnerable to Attack

OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

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

September 23, 2025

MEMORANDUM FOR: Benjamine C. Huffman
Senior Official Performing the Duties of the
Under Secretary for Management

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

JOSEPH V CUFFARI
Digitally signed by JOSEPH V CUFFARI
Date: 2025.09.22 09:19:23 -07'00'

SUBJECT: *Inadequate Cybersecurity Rendered DHS Headquarters High-Value System Vulnerable to Attack*

Attached for your action is our final report, *Inadequate Cybersecurity Rendered DHS Headquarters High-Value System Vulnerable to Attack*. We incorporated the formal comments provided by your office.

The report contains five recommendations aimed at improving DHS Headquarters' ability to secure its High Value Asset system. Your office concurred with all five recommendations. Based on information provided in your response to the draft report, we consider recommendations 1 through 5 open and resolved. Once your office has fully implemented the recommendations, please submit a formal closeout letter to us within 30 days so that we may close the recommendations. 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 Craig Adelman, Deputy Inspector General, Office of Audits, at (202) 981-6000.

Attachment

DHS OIG HIGHLIGHTS

Inadequate Cybersecurity Rendered DHS Headquarters High-Value System Vulnerable to Attack

September 23, 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 DHS HQ has implemented effective technical controls to protect sensitive information on a selected HVA system.

What We Recommend

We made five recommendations to improve DHS HQ's ability to secure its HVA system.

For Further Information:
Contact OIG Public Affairs at (202) 981-6000 or DHS-OIG.OfficePublicAffairs@oig.dhs.gov.

What We Found

The Department of Homeland Security Headquarters (HQ) did not adequately secure a non-Tier 1 High Value Asset (HVA) system used to support data analysis and reporting on DHS component operations, which rendered the system and its sensitive information vulnerable to cyberattacks.

Although DHS HQ developed policies and procedures meant to reduce risks to sensitive information stored on the HVA system and effectively implemented certain controls, we determined the system did not meet security requirements.

We identified nine unique critical and high-risk vulnerabilities that appeared 182 times in the system and, through simulated cyberattack penetration testing, were able to exploit vulnerabilities. The vulnerabilities we identified pose significant security risks, increasing the likelihood an attacker could gain access to sensitive information.

These deficiencies demonstrate that DHS HQ needs to strengthen its management of the HVA system. Ensuring the system complies with the Department's security and privacy policies will better protect the sensitive information processed by the system. Until these deficiencies are addressed, DHS HQ may not be equipped to protect the HVA system and cannot ensure it will be able to quickly respond to and recover from a cyberattack.

DHS HQ Response

DHS HQ concurred and has begun taking action to address all five recommendations. Appendix B contains DHS HQ's management comments in their entirety.

Table of Contents

Abbreviations

API	application programming interface
ATO	authority to operate
FISMA	*Federal Information Security Modernization Act of 2014*
HQ	headquarters
HVA	High Value Asset
ICR	inventory change request
MFA	multifactor authentication
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
SP	Special Publication
STIG	Security Technical Implementation Guide
U.S.C.	United States Code

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]

To protect mission continuity, the Office of Management and Budget (OMB) created the High Value Asset (HVA) security initiative in 2015,[2] requiring large Federal agencies to identify their most critical assets. Across the Federal Government, agencies operate HVAs that contain sensitive information and support critical services. HVAs include Federal information systems, information, and data for which unauthorized access, use, disclosure, disruption, modification, or destruction could cause a significant impact to national security interests, foreign relations, the economy, safety, and the security of the American people.

In 2018, OMB issued additional guidance for agencies to designate information or an 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.[3] As part of its cybersecurity responsibilities, the Cybersecurity and Infrastructure Security Agency categorizes HVAs as either Tier 1 or non–Tier 1, based on criticality and impact. Tier 1 systems have a critical impact on both the agency and the Nation, and non–Tier 1 systems have a significant impact on both the agency and the Nation. For this review, we selected one of DHS Headquarters' (HQ) cloud-based non-Tier 1 HVA systems (hereafter referred to as the "HVA system").

We conducted this review to determine whether DHS HQ has implemented effective technical controls to protect sensitive information on a selected HVA system.[4]

Results of Review

DHS HQ did not effectively implement technical controls for the HVA system per Federal and departmental requirements, including National Institute of Standards and Technology (NIST)

[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] OMB M-19-03, *Strengthening the Cybersecurity of Federal Agencies by enhancing the High Value Asset Program,* December 10, 2018.
[4] We are not identifying the system by name in this report to protect sensitive information on the HVA system. The system is used to support data analysis and reporting on DHS component operations.

Special Publication (SP) 800-53, *Security and Privacy Controls for Information Systems and Organizations,* and DHS Policy Directive 4300A, *Information Technology System Security Program, Sensitive Systems,* February 13, 2023. DHS HQ developed policies and procedures meant to reduce risks to sensitive information stored on the HVA system and effectively implemented certain controls. However, we identified security deficiencies in six of the nine NIST control families tested. Specifically, we identified deficiencies in:

- risk assessment;
- configuration management;
- identification and authentication;
- access control;
- awareness and training; and
- incident response.

These deficiencies demonstrate that DHS HQ needs to strengthen its management of the HVA system. Ensuring the system complies with the Department's security and privacy policies will better protect the sensitive information processed by the system. Until these deficiencies are addressed, DHS HQ may not be equipped to protect the HVA system and cannot ensure it will be able to quickly respond to and recover from a cyberattack.

DHS HQ Did Not Effectively Implement Security and Privacy Controls to Protect Sensitive Information Processed by the HVA System

DHS HQ did not effectively implement security and privacy controls for the HVA system per Federal and departmental requirements. Specifically, DHS HQ did not effectively implement the required security and privacy controls to protect the sensitive information stored and processed by the HVA in six of the nine NIST SP 800-53 control families tested, as shown in Table 1.[5]

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

Table 1. Deficiencies Identified in NIST SP 800-53 Control Families Tested and Corresponding Functions in the NIST Cybersecurity Framework[6]

NIST SP 800-53		NIST Cybersecurity Framework	
Control Family Tested	Deficiencies Identified	Function	FISMA[7] Domain
Risk Assessment	Yes	Identify	Risk Management
Configuration Management	Yes	Protect	Configuration Management
Assessment, Authorization, and Monitoring	No	Detect	Information Security Continuous Monitoring
Identification and Authentication	Yes	Protect	Identity and Access Management
Access Control	Yes	Protect	Data Protection and Privacy
Awareness and Training	Yes	Protect	Security Training
Planning (Rules of Behavior)	No	Protect	Identity and Access Management
Audit and Accountability	No	Protect	Data Protection and Privacy
Incident Response	Yes	Respond	Incident Response

Source: Compiled by DHS OIG based on NIST SP 800-53 Revision 4 and Revision 5, NIST Cybersecurity Framework, and fiscal year 2024 FISMA reporting metrics[8]

[6] NIST, v1.1, *Framework for Improving Critical Infrastructure Cybersecurity*, April 16, 2018.
[7] *Federal Information Security Modernization Act of 2014* (FISMA), Pub. L. No. 113-283, 44 U.S.C. § 3551 et. seq.
[8] NIST 800-53 Revision 5 controls applied to the HVA system before DHS migrated the system to the cloud in December 2023. Although NIST 800-53 Revision 4 was rescinded upon NIST's issuance of Revision 5 in September 2020, DHS systems inheriting controls from a cloud service provider were not authorized by the FedRAMP Joint Authorization Board to adopt Revision 5 controls during our fieldwork. For controls we tested using data prior to the HVA system's cloud migration, we used Revision 5. For any controls we tested using data following the HVA system's cloud migration, we used Revision 4.

Control Family – Risk Assessment

DHS HQ Did Not Effectively Patch Critical and High-Severity Vulnerabilities

DHS HQ did not ensure all known software updates were promptly applied to the HVA system's servers and workstations. DHS policy[9] requires system owners to remediate software vulnerabilities within specified timeframes. Through our vulnerability assessments of the HVA system, we identified nine unique critical and high-risk vulnerabilities that appeared 182 times in the system's development and production environments that should have been remediated. This total included five unique types of critical vulnerabilities and four unique types of high-risk vulnerabilities. DHS HQ did not address the vulnerabilities within DHS' specified remediation compliance timeframes, per guidance published by the DHS Enterprise Security Operations Center. For example, one high-risk vulnerability identified on May 23, 2024, had not been remediated since the related patch was released in August 2023. Table 2 shows the results of our vulnerability assessment.

Table 2. Vulnerability Assessment Results

System Environment	Unique Critical Vulnerabilities	Unique High-Risk Vulnerabilities	Critical Vulnerability Instances	High-Risk Vulnerability Instances
Development[10]	2	2	20	34
Production[11]	3	2	60	68
Total	5	4	80	102

Source: DHS OIG technical testing

The vulnerabilities we identified occurred because DHS HQ did not appropriately apply software patches. Using unpatched software increases the risk that a malicious actor could negatively impact or compromise the HVA system environment.

[9] DHS Policy Directive 4300A, v16, *Sensitive Systems Handbook, Attachment O, Vulnerability Management,* August 1, 2022.
[10] A development environment is a controlled workspace used by developers to write, test, and debug code being used for an application before making it available to the public.
[11] A production environment is the live and latest version of a software or application that is accessible to the end user.

Control Family – Configuration Management

DHS HQ Developed Configuration Management Policies and Procedures but Did Not Ensure the HVA System Complied with Required Configuration Settings

DHS HQ developed configuration management policies and procedures for the HVA system, as required. DHS policy[12] requires information security patches to be installed in accordance with component configuration management plans, following the timeline for remediating software vulnerabilities. DHS HQ's configuration management policies and procedures outlined system patching guidance for the HVA system.[13]

Across the seven servers that host the HVA system's development and production environments, our configuration compliance scans discovered 326 noncompliant settings related to the Defense Information Systems Agency Security Technical Implementation Guides (STIG), resulting in an overall compliance score of 89 percent. For example, the HVA system did not:

- require users to provide a password for privilege escalation;[14]
- require users to periodically change their passwords;
- adequately prohibit the use of cached authentications;[15] and
- implement smartcard login for multifactor authentication (MFA) to access interactive accounts.[16]

The system owner stated STIG compliance scores are constantly changing and acknowledged their point-in-time compliance score of 89 percent. The system remains vulnerable to cyberattacks until the STIG requirements are fully implemented.

DHS OIG Successfully Exploited Security Weaknesses in the HVA System

Using penetration testing, we identified exploitable vulnerabilities through simulated cyberattacks. We tested the HVA system for 10 industry-recognized vulnerabilities[17] and found it was not properly configured and was using an outdated software version containing a well-

[12] DHS Policy Directive 4300A, v13.3, *Information Technology System Security Program, Sensitive Systems*, February 13, 2023.
[13] *Cloud Services Branch – Amazon Web Services (AWS), Operating System (OS) Layer Patch Management Standard Operating Procedure (SOP)*, December 20, 2023.
[14] Privilege escalation is a cyberattack designed to gain unauthorized privileged access into a system.
[15] Cached authentication is a security mechanism that stores user credentials on a local device that allows a user to log in even if the network or domain controller is unavailable.
[16] Interactive accounts are accounts that can help users gain access to the systems and run programs with the use of a password.
[17] The Open Worldwide Application Security Project Top 10 presents an industry consensus about the most critical security risks to web applications.

known vulnerability. DHS policy[18] requires that systems are fully patched and in compliance with DHS configuration guidance. The policy also requires continuous monitoring through the review of current vendor patch notifications, security configuration best practices, security architecture guidance, and emerging threats and vulnerabilities.

The HVA system owner acknowledged the vulnerabilities and suggested remediation patches may have been applied during the following month's patching cycle. The vulnerabilities we identified pose significant security risks, increasing the likelihood an attacker could gain access to sensitive information.

DHS HQ Did Not Update the Department's System Inventory to Reflect the HVA's Cloud Migration

DHS HQ did not file an inventory change request (ICR) form before migrating the HVA to the cloud, as required. NIST 800-53 Revision 4[19] requires organizations to maintain accurate inventories of system components, including hardware, software, firmware, and any information deemed necessary for system component accountability. DHS policy[20] also requires organizations to follow an established change management process to maintain the integrity of the Department's FISMA system inventory. DHS' change management process requires system owners to submit ICR forms throughout system development lifecycle phases, establishing an audit trail for all Department information system changes. System stakeholders acknowledged the oversight and subsequently filed the ICR on February 16, 2024.

Control Family – Assessment, Authorization, and Monitoring

DHS HQ Did Not Reassess the Authority to Operate for the HVA's Cloud Migration

DHS HQ did not reassess its authority to operate (ATO) for the HVA system when it moved to the cloud environment in December 2023. However, the system had an ATO for its on-premises servers until April 2025 that the DHS Office of the Chief Information Security Officer confirmed was still valid. DHS policy[21] requires an authorizing official to grant an ATO before an information system first becomes operational and to reauthorize the system when changes are made that affect the potential level of operational risk.

[18] DHS Policy Directive 4300A, v16, *Sensitive Systems Handbook,* Attachment O, August 1, 2022.
[19] NIST SP 800-53 Revision 4, *CM-8 Information System Component Inventory,* April 2013. See Footnote 8.
[20] DHS Policy Directive 4300A, v15, *Information Technology System Security Program*, Attachment DD, January 26, 2023.
[21] DHS *System Security Authorization Process Guide*, v14.1, April 4, 2019.

Control Family – Identification and Authentication

DHS HQ Did Not Implement Multifactor Authentication Across All HVA's Environments

DHS OIG assessed DHS HQ's use of MFA for standard user accounts, database accounts, and application programming interface (API) privileged and nonprivileged user accounts across the HVA's development and production environments. NIST 800-53 Revision 5[22] requires agencies to uniquely identify and authenticate organizational users, and DHS policy[23] requires that sensitive systems be protected by strong authentication. According to the policy directive, DHS achieves strong authentication by using MFA.

DHS implemented MFA but did not utilize it for all user accounts. Through testing, we verified that all database user accounts required username and password authentication and API accounts required a customer ID and password. DHS officials explained that users initially access the HVA system using a form of MFA, personal identity verification credentials. However, the officials acknowledged that the HVA system used only username and password authentication for API user accounts and database administrator accounts. The lack of MFA for these accounts makes it easier for an attacker to compromise the system and gain unauthorized access to sensitive data stored within.

Control Family – Access Control

DHS HQ Did Not Provide Evidence of User Account Reviews

DHS HQ officials could not provide evidence that the HVA system's user accounts were reviewed, as required. NIST 800-53 Revision 4[24] requires agencies to authorize system access according to agency-defined policies and procedures. Additionally, DHS Directive 4300A[25] requires system owners to review information system accounts annually and when significant changes occur to the system environment. The system owner stated they conduct informal user account reviews approximately every 6 months. However, this process was not documented, and DHS was unable to provide evidence of completed reviews. Without a formal, documented process for regular system access reviews, DHS HQ risks unauthorized access to sensitive data.

[22] NIST SP 800-53, Revision 5, *IA-2 Identification and Authentication (Organizational Users),* September 2020.
[23] DHS Policy Directive 4300A, v13.3, *Information Technology System Security Program, Sensitive Systems*, February 13, 2023.
[24] NIST SP 800-53 Revision 4, *AC-2 Account Management,* April 2013.
[25] DHS Policy Directive 4300A, v13.3, *Information Technology System Security Program, Sensitive Systems*, February 13, 2023.

Control Family – Awareness and Training

DHS HQ Did Not Provide Evidence that System Users Had Taken Required Cybersecurity Awareness and Role-Based Training Courses

DHS HQ could not demonstrate that all the HVA system's privileged users completed the required cybersecurity training courses. Program officials said they were unable to produce some users' training records because the records were lost when the Department decommissioned its enterprise learning management system in August 2023. Federal regulation,[26] along with directives from OMB[27] and DHS, mandate annual security awareness training for employees and contractors. This training aims to educate users on information security risks, risk mitigation strategies, and their security responsibilities. The DHS directive and NIST 800-53 Revision 5[28] require personnel with elevated privileges to complete specialized, role-based training before accessing systems containing sensitive information, and annually thereafter. The DHS directive also requires components to maintain records of system users' training to track and enforce these training requirements.

We reviewed FY 2023 training records for each of the HVA system's 20 privileged users. DHS could not provide evidence of completed cybersecurity awareness training for 3 of the 20 users. Similarly, DHS could not provide evidence of completed privileged user training for 3 of the 20 users. Lastly, DHS could not provide evidence of completed role-based training for 18 of the 20 users. The inability to track user course completion prevents DHS from ensuring privileged users of the HVA system are aware of critical cybersecurity concepts and from taking action against noncompliant user accounts.

Control Family – Incident Response

DHS HQ Did Not Finalize Its Incident Response Plan for the HVA

NIST 800-53 Revision 4[29] requires agencies to develop, review, and approve an incident response plan for their systems. We determined the HVA system went without an approved plan between February and April 2024. DHS HQ provided the evaluation team with a draft incident response plan for the HVA system, but it was not finalized or approved. DHS HQ officials stated that the plan was undergoing a periodic review process during our testing. DHS finalized the system's incident response plan in April 2024, while our review was ongoing.

[26] FISMA, Pub. L. No. 113-283, 44 U.S.C. § 3551 et. seq.
[27] OMB Circular A-130, *Managing Information as a Strategic Resource,* July 28, 2016.
[28] NIST 800-53, Revision 5, *AT-2 Literacy Training and Awareness* and *AT-3 Role-Based Training,* September 2020.
[29] NIST 800-53, Revision 4, *IR-8 Incident Response Plan,* April 2013. See Footnote 8.

Conclusion

Although DHS HQ implemented some of the security and privacy controls tested, we identified several areas for improvement. Without effective security patch application and configuration management implementation, DHS HQ cannot ensure the protection and security of sensitive information processed by the HVA system we reviewed. Also, without effective system access controls, including MFA, DHS HQ cannot protect against unauthorized users. Finally, by not ensuring system users are properly trained, DHS HQ increases the risk of security or privacy incidents resulting from human error. Until these deficiencies are addressed, DHS HQ is less equipped to protect the HVA system and ensure a timely response and recovery from a cyberattack.

Recommendations

Recommendation 1: We recommend the DHS Office of the Chief Information Officer require the High Value Asset system owner to apply security updates and software patches to remediate vulnerabilities on all devices in accordance with applicable DHS policies.

Recommendation 2: We recommend the DHS Office of the Chief Information Officer require the High Value Asset system owner to perform configuration testing and verify that all approved settings are implemented.

Recommendation 3: We recommend the DHS Office of the Chief Information Officer require the High Value Asset system owner to implement multifactor authentication for all database and application programming interface accounts.

Recommendation 4: We recommend the DHS Office of the Chief Information Officer direct the High Value Asset system owner to ensure user accounts are reviewed annually.

Recommendation 5: We recommend the DHS Office of the Chief Information Officer confirm the current enterprise learning management system adequately retains documentation to demonstrate users' compliance with security awareness training, privileged user training, and role-based training.

Management Comments and OIG Analysis

DHS HQ provided written comments in response to the draft report and concurred with all five recommendations. Appendix B contains DHS HQ's management comments in their entirety. We also received technical comments from DHS HQ on the draft report and revised the report as appropriate. We consider all five recommendations open and resolved. A summary of DHS HQ's response and our analysis follows.

DHS HQ Response to Recommendation 1: Concur. According to DHS HQ, all vulnerabilities we identified during testing were addressed through security updates and software patches as of June 26, 2024. Additionally, DHS implemented various processes in accordance with departmental policy to ensure critical vulnerabilities are remediated within 21 days of discovery and high-risk vulnerabilities are addressed within 30 days of discovery. Further, system engineers now perform routine change requests monthly to manage patching and software updates, and security updates and software patches are executed by two teams — a platform team and an application team. Each team conducts monthly updates during separate patching cycles. To maintain the security and integrity of the system, the DHS Office of the Chief Information Officer will continue to monitor the system through weekly vulnerability scans, as appropriate. DHS provided us with a presentation detailing these efforts on June 12, 2025.

OIG Analysis: These actions are responsive to the recommendation, which we consider open and resolved. Once DHS HQ provides evidence that the scans have addressed all identified vulnerabilities, we will close the recommendation.

DHS HQ Response to Recommendation 2: Concur. According to DHS HQ, configuration settings are verified through weekly configuration scans. Additionally, new servers are provisioned using DHS-approved STIG images, which are scanned for potential misconfigurations. For "Category 1" STIG misconfigurations (i.e., major configuration issues), remediation efforts are tracked via service tickets submitted to the DHS Enterprise Cloud Amazon Web Services team.

The DHS Office of the Chief Information Officer Solution Development Directorate's DHS Enterprise Cloud platform team continuously updates configuration management requirements to align with DHS configuration management guidance, as published on its Sensitive Systems Configuration Guidance intranet page. DHS provided us with a presentation detailing these efforts on June 12, 2025.

OIG Analysis: These actions are responsive to the recommendation, which we consider open and resolved. We will close the recommendation when DHS HQ provides evidence demonstrating STIG compliance for the settings we identified.

DHS HQ Response to Recommendation 3: Concur. The Office of the Chief Information Officer, in collaboration with HVA system owners, is exploring a technical approach to address this recommendation. This review is expected to be completed by the second quarter of FY 2026. Given the potential impact on current program planning and anticipated technical changes, the system program manager is reviewing the cost, scope, and feasibility of remediating this finding. Once this review is complete, DHS leadership will evaluate the results and determine the most appropriate path forward. Estimated Competition Date: August 31, 2026.

OIG Analysis: These actions are responsive to the recommendation, which we consider open and resolved. We will close the recommendation when DHS HQ provides evidence that MFA has been implemented for all database and API accounts.

DHS HQ Response to Recommendation 4: Concur. According to DHS HQ, the Office of the Chief Information Officer has conducted three quarterly user account reviews as of August 2025. These processes are documented, maintained, and tracked on the DHS HQ Confluence site and within the Cybersecurity Assessment and Management system. DHS provided us with a presentation detailing these efforts on June 12, 2025.

OIG Analysis: These actions are responsive to the recommendation, which we consider open and resolved. We will close the recommendation when DHS HQ provides evidence that the processes are on the Confluence site and that the quarterly user account reviews address the HVA system users.

DHS HQ Response to Recommendation 5: Concur. According to DHS HQ, training status is documented and tracked at both the individual and role levels. Training records are maintained in the DHS HQ Online Learning Management and Education System, which became operational on July 8, 2024. These records include cybersecurity awareness training, privileged user training, and role-based training. Before provisioning access to the system, all required training certificates are submitted to the infrastructure team to validate that the user's training is current. DHS provided us with a presentation detailing these efforts on June 12, 2025.

OIG Analysis: These actions are responsive to the recommendation, which we consider open and resolved. We will close the recommendation when DHS HQ provides evidence that the training records are retained in the Learning Management and Education System.

Appendix A:
Objective, Scope, and Methodology

Our objective was to determine whether DHS HQ has implemented effective technical controls to protect sensitive information on the HVA system. We focused our review on one DHS HQ HVA system. To accomplish our objective, we determined whether DHS HQ had effective controls in the following areas:

- risk assessment;
- configuration management;
- assessment, authorization, and monitoring;
- identification and authentication;
- access control;
- awareness and training;
- planning (rules of behavior);
- audit and accountability; and
- incident response.

We interviewed DHS HQ officials and reviewed DHS HQ's documentation and data for the selected HVA system to evaluate their implementation of selected NIST SP 800-53 Revision 4 and Revision 5 controls. We selected all HVA system users for testing in the areas of user account management, security awareness training, and role-based training. We conducted technical assessments to identify potential vulnerabilities, missing patches, and noncompliance with Defense Information Systems Agency STIG configuration settings. To ensure the accuracy of testing results and DHS OIG reporting, DHS HQ reviewed our preliminary observations and identified false-positive results, as applicable. We reviewed DHS HQ's feedback and updated our analysis as necessary. 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 January 2024 and March 2025, under the authority of the *Inspector General Act of 1978*, as amended, 5 U.S.C. §§ 401–424, and according to the *Quality Standards for Inspection and Evaluation*, issued by the Council of the Inspectors General on Integrity and Efficiency.

DHS OIG's Access to DHS Information

During this review, DHS OIG experienced a significant delay to the start of its technical testing in 2024. The delay was caused by DHS' reluctance to sign a Rules of Engagement agreement with DHS OIG. The Inspector General reported this delay to the DHS Secretary before it was resolved.

Appendix B:
DHS HQ Comments on the Draft Report

U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

BY ELECTRONIC SUBMISSION

August 19, 2025

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

FROM: Jeffrey M. Bobich
Director of Financial Management

JEFFREY M BOBICH
Digitally signed by JEFFREY M BOBICH
Date: 2025.08.19 08:53:33 -04'00'

SUBJECT: Management Response to Draft Report: "Inadequate Cybersecurity Rendered DHS Headquarters High-Value System Vulnerable to Attack"
(Project No. 24-008-AUD-DHS)

Thank you for the opportunity to comment on this draft report. The U.S. Department of Homeland Security (DHS, or the Department) appreciates the work of the Office of Inspector General (OIG) in planning and conducting its review and issuing this report.

DHS leadership is pleased to note OIG's recognition of the Department's efforts to reduce risks to sensitive information stored on the High Value Asset system, such as DHS developing policies and procedures and effectively implementing certain controls. DHS remains committed to maintaining a strong information security program and implementing practices that ensure the Department effectively protects the information and systems supporting DHS operations and assets.

It is important to note that DHS believes the OIG's characterization of the Department as being reluctant to sign a Rules of Engagement agreement is inaccurate and lacks critical context. Specifically, from February to May 2024, the Office of the Chief Information Officer engaged with the OIG to address questions, discuss roles and responsibilities, and avoid redundancy in testing. Accordingly, it is important that readers understand this was a result of the Department's commitment to ensuring thorough review and coordination before finalizing the Rules of Engagement, rather than reluctance to engage.

The draft report contained five recommendations, with which the Department concurs. Enclosed find our detailed response to each recommendation. DHS 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

Attachment: Management Response to Recommendations Contained in OIG 24-008-AUD-DHS

OIG recommended the DHS Office of the Chief Information Officer:

Recommendation 1: Require the [High Value Asset] system owner to apply security updates and software patches to remediate vulnerabilities on all devices in accordance with applicable DHS policies.

Response: Concur. As of June 26, 2024, all vulnerabilities identified by OIG during testing were addressed through security updates and software patches. Additionally, DHS implemented various processes in accordance with Departmental policy[1] to ensure timely patching and remediation of vulnerabilities. Under the current process, critical vulnerabilities are remediated within 21 days, and high vulnerabilities are addressed within 30 days of discovery.

Further, system engineers now perform routine change requests on a monthly basis to manage patching and software updates, and security updates and software patches are executed by two teams—a platform team and an application team. Each team conducts monthly updates during separate patching cycles. To maintain the security and integrity of the system, the DHS Office of the Chief Information Officer will continue to monitor the system through weekly vulnerability scans, as appropriate. DHS provided OIG with a presentation detailing these efforts on June 12, 2025.

DHS requests that the OIG consider this recommendation resolved and closed, as implemented.

Recommendation 2: Require the [High Value Asset] system owner to perform configuration testing and verify that all approved settings are implemented.

Response: Concur. Configuration settings are verified through weekly configuration scans. Additionally, new servers are provisioned using DHS-approved Security Technical Implementation Guide[2] images, which are scanned for potential misconfigurations. For "Category 1" Security Technical Implementation Guide

[1] DHS 4300A V13.4, "DHS Policy Directive, Information Technology System Security Program, Sensitive Systems" dated December 6, 2024, establishes the baseline requirements for the secure operation of information systems within the Department of Homeland Security. It provides guidance to ensure the confidentiality, integrity, and availability of DHS systems and data.
[2] A Security Technical Implementation Guide is a configuration standard that provides cybersecurity guidance for hardening information systems and software. These guides outline specific technical settings to reduce vulnerabilities and ensure compliance with federal cybersecurity regulations.

misconfigurations[3] (major configuration issues), remediation efforts are tracked via service tickets submitted to the DHS Enterprise Cloud Amazon Web Services team.

The DHS Office of the Chief Information Officer Solution Development Directorate's DHS Enterprise Cloud platform team continuously updates configuration management requirements to align with DHS configuration management guidance, as outlined in the Sensitive Systems Configuration Guidance.[4] DHS provided OIG with a presentation detailing these efforts on June 12, 2025.

DHS requests that the OIG consider this recommendation resolved and closed, as implemented.

Recommendation 3: Require the [High Value Asset] System owner to implement multifactor authentication for all database and API [application programming interface] accounts.

Response: Concur. The Office of the Chief Information Officer, in collaboration with High Value Asset system owners, is actively exploring a technical approach to address this recommendation. This review is expected to be completed by the second quarter of fiscal year 2026. Given the potential impact on current program planning and anticipated technical changes, the system program manager is conducting a thorough review of cost, scope, and the feasibility to remediate this finding. Once this review is complete, DHS leadership will evaluate the results and determine the most appropriate path forward. Estimate Competition Date: August 31, 2026.

Recommendation 4: Direct the [High Value Asset] system owner to ensure user accounts are reviewed annually.

Response: Concur. As of August 2025, the Office of the Chief Information Officer has conducted three quarterly user account reviews. These processes are now fully documented, maintained, and tracked on the DHS Headquarters Confluence site and within the Cybersecurity Assessment and Management system. DHS provided OIG with a presentation detailing these efforts on June 12, 2025.

DHS requests that the OIG consider this recommendation resolved and closed, as implemented.

Recommendation 5: Confirm the current enterprise learning management system adequately retains documentation to demonstrate user compliance with security

[3] Category 1 within the DHS Security Technical Implementation Guides refers to vulnerabilities that pose the highest level of risk. These vulnerabilities could result in the loss of confidentiality, integrity, or availability of systems, leading to catastrophic consequences for the organization or mission.
[4] "DISA Security Technical Implementation Guide Red Hat Enterprise Linux 8 v2r3,". dated May 20, 2025.

awareness training, privileged user training, and role-based training.

Response: Concur. Training status is documented and closely tracked at both the individual and role levels. Training records are maintained in the DHS Headquarters Online Learning Management & Education System, which became operational on July 8, 2024. These records include cybersecurity awareness training, privileged user training, and role-based training. Before provisioning access to the system, all required training certificates are submitted to the infrastructure team to validate that the user's training is current. DHS provided OIG with a presentation detailing these efforts on June 12, 2025.

DHS requests that the OIG consider this recommendation resolved and closed, as implemented.

5

Appendix C:
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
OCIO, DHS HQ
Audit Liaison, DHS HQ

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