OFFICE OF INSPECTOR GENERAL

CBP Implemented Effective Technical Controls to Secure a Selected Tier 1 High Value Asset System

Homeland Security

August 23, 2023

OIG-23-43

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

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

August 23, 2023

MEMORANDUM FOR: Troy Miller
Deputy Commissioner and Senior Official Performing the Duties of the Commissioner
U.S. Customs and Border Protection

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

JOSEPH V CUFFARI
Digitally signed by JOSEPH V CUFFARI
Date: 2023.08.22 17:05:43 -04'00'

SUBJECT: *CBP Implemented Effective Technical Controls to Secure a Selected Tier 1 High Value Asset System*

For your action is our final report, *CBP Implemented Effective Technical Controls to Secure a Selected Tier 1 High Value Asset System*. Your office chose not to submit management comments to the draft report. The report contains no recommendations.

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, Acting Deputy Inspector General for Audits, at (202) 981-6000.

Attachment

DHS OIG HIGHLIGHTS

CBP Implemented Effective Technical Controls to Secure a Selected Tier 1 High Value Asset System

August 23, 2023

Why We Did This Review

Across the Federal Government, various departments including DHS, operate HVA systems that contain sensitive information and/or support critical services. We conducted this review to determine whether CBP implemented effective technical controls to protect the sensitive information that is stored and processed by a selected HVA system.

What We Recommend

We did not make recommendations to address the deficiencies identified because CBP retired the HVA and migrated the system from a server to a cloud-based environment.

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

Components within the Department of Homeland Security protect High Value Asset (HVA) systems with security and privacy controls designed to keep sensitive information safe. We determined that U.S. Customs and Border Protection (CBP) implemented most security and privacy controls tested for the selected HVA system, in compliance with applicable Federal and DHS requirements. We identified deficiencies in 2 of 10 control families — Configuration Management and Supply Chain Risk Management (SCRM). Specifically, CBP did not have waivers or risk acceptance letters for noncompliant configuration management settings, but we determined the overall compliance rate was effective.

Additionally, CBP did not implement a system-level SCRM plan as recommended by the most recent National Institute of Standards and Technology (NIST) guidance and required by the Office of Management and Budget. This occurred because DHS delayed development and publication of its department-level guidance instructing components to adopt the NIST controls, including system-level SCRM plans.

Although CBP implemented most controls for the selected HVA system and remediated vulnerabilities in the HVA databases, until the Federal Government and DHS implement SCRM controls, agencies cannot be assured that sensitive information stored and processed by HVA systems is fully protected and secure.

CBP Response

CBP agreed with the report and chose not to submit formal management comments but provided technical comments, which we incorporated as appropriate.

Background

The United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people's security and privacy. The use of information technology (IT) systems and data can also introduce risk in an increasingly digital and mobile environment. In recent years, the Federal Government has seen an increase in the number of information security incidents affecting the integrity, confidentiality, and/or availability of Government information, systems, and services. The Department of Homeland Security (DHS) Office of Inspector General (OIG) and the U.S. Government Accountability Office (GAO) have both identified preventing cyberattacks as a major management and performance challenge.[1] In response to these threats, the President directed the Federal Government to improve its efforts to identify, deter, protect against, detect, and respond to these actions and actors.[2]

To specifically protect mission continuity, the Office of Management and Budget (OMB) created the High Value Asset (HVA) security initiative in 2015, which required large Federal agencies to identify their most critical assets.[3] Across the Federal Government, agencies operate HVAs that contain sensitive information and/or 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.[4]

In 2018, OMB issued additional guidance for agencies to designate information and/or an information system as an HVA when it is related to any of the following categories: informational value, mission essential, or Federal civilian enterprise essential.[5] The Cybersecurity and Infrastructure Security Agency categorizes HVAs as Tier 1 and 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.

Several guidelines and best practices are in place to help Federal agencies manage security risks and protect their information systems, including HVAs. For example, the National Institute of Standards and Technology (NIST) provides

[1] *Department of Homeland Security's Annual Performance Report (APR) for FY 2021-2023*.
[2] Executive Order 14028, *Improving the Nation's Cybersecurity*, May 17, 2021.
[3] OMB M-16-03, *Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirement*, October 30, 2015.
[4] OMB M-17-09, *Management of Federal High Value Assets*, December 9, 2016.
[5] OMB M-19-03, *Strengthening the Cybersecurity of Federal Agencies by Enhancing the High Value Asset Program*, December 10, 2018.

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).[6]

NIST also develops guidance for categorizing and protecting Federal information and systems according to risk levels. For instance, NIST Special Publication (SP) 800-53 Revision 5[7] provides guidance for selecting security controls to achieve more secure information systems and effective risk management within the Federal Government. Similarly, the *Federal Information Security Modernization Act of 2014* (FISMA) requires each Federal agency to develop, document, and implement an enterprise-wide cybersecurity program to protect its systems and data. The DHS Office of Inspector General is responsible for conducting annual evaluations of DHS information programs and systems.

U.S. Customs and Border Protection (CBP) is one of the world's largest law enforcement organizations and is charged with protecting our Nation's border and facilitating lawful international travel and trade. As the United States' first unified border entity, CBP uses a comprehensive approach for border management, which includes customs, immigration, border security, and agricultural protection.

We conducted this review as part of our FISMA oversight to determine whether CBP implemented effective technical controls to protect the sensitive information processed by a selected HVA system. For this review, we randomly selected one of CBP's Tier 1 HVA systems (hereafter referred to as the HVA system). At the time of our review, the HVA system was server-based and housed in Virginia. CBP designated the HVA system as Tier 1 and categorized it with an overall Security Categorization[8] as "High," including "High" for all three security objectives (Confidentiality, Integrity, and Availability). This report is one in a series on the Department's HVAs. We plan to incorporate the results from this review into our fiscal year 2023 FISMA submission.

Results of Review

CBP implemented most security and privacy controls tested for the selected HVA system, in compliance with applicable Federal and departmental

[6] *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1, April 16, 2018.
[7] NIST SP 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, September 2020.
[8] Federal Information Processing Standards 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004, establishes security categories for both information and information systems. The security categories are based on the potential impact on an organization in accomplishing its assigned mission, protecting its assets, fulfilling its legal responsibilities, or maintaining its day-to-day functions when certain events occur that may affect the information and information systems needed by the organization.

requirements. We identified deficiencies in 2 of 10 control families — Configuration Management and Supply Chain Risk Management (SCRM). Specifically, CBP did not have waivers or risk acceptance letters for noncompliant configuration management settings, but we determined the overall compliance rate was effective. Additionally, CBP did not implement a system-level SCRM plan as recommended by NIST SP 800-53 Rev. 5 and required by OMB.[9] This occurred because DHS delayed development and publication of its department-level guidance instructing components to adopt NIST SP 800-53 Rev. 5 controls, including system-level SCRM plans.[10] Although CBP implemented most controls for the selected HVA system and remediated vulnerabilities in the HVA databases, until the Federal Government and DHS implement SCRM controls, agencies cannot be assured that sensitive information stored and processed by HVA systems is fully protected and secure. We did not make recommendations to address the deficiencies identified because CBP retired the HVA and migrated the system from a server to a cloud-based environment.

CBP Implemented Most Controls to Protect Sensitive Information Stored on the Selected HVA System

We reviewed controls designed to protect sensitive information stored and processed by the selected HVA system and found that CBP implemented most of them, as shown in Table 1, and further described in Appendixes A and B.

Table 1. CBP Compliance with NIST SP 800-53 Controls Tested

Control Family	Controls Effective	Deficiencies Identified
(1) Configuration Management*	☑*	Yes
(2) Risk Assessment	☑	No
(3) Supply Chain Risk Management	☒	Yes
(4) Access Controls	☑	No
(5) Planning	☑	No
(6) Awareness and Training	☑	No
(7) Assessment, Authorization, and Monitoring	☑	No
(8) Contingency Planning	☑	No
(9) Incident Response	☑	No
(10) Audit and Accountability	☑	No

Source: DHS OIG analysis

[9] OMB Circular A-130, *Managing Information as a Strategic Resource*, July 28, 2016.
[10] *DHS MGMT-HQ Component Level Migration Plan*, March 29, 2023.

*We determined CBP's overall configuration management controls were effective despite finding deficiencies in 6 of 471 settings.

CBP Implemented Most Controls, But We Identified Deficiencies

Although CBP implemented most NIST controls tested, we identified deficiencies in the configuration management and SCRM control families. For configuration management, we identified noncompliant settings and determined CBP did not have waivers or risk acceptance letters for the associated controls. For SCRM, we determined CBP did not develop a system-level SCRM plan.

We assessed CBP's configuration management settings for its HVA system and determined CBP implemented effective configuration management controls. Overall, CBP was about 99 percent compliant in implementing effective configuration management controls. Although we consider CBP's level of compliance effective, we found CBP did not implement 6 of the 471 required baseline configuration settings. Before our review ended, CBP implemented one of six missing controls. Although CBP is authorized to accept the risk, it was not able to provide approved waivers or risk acceptance letters for the missing controls. Table 2 summarizes CBP's compliance with DHS-required baseline configuration settings.

Table 2. Configuration Management Assessment Results

Operating System	Assets Scanned	Compliance Percentage
Server Group One	11	99%
Server Group Two	38	99%
Total	**49**	**--**

Source: DHS OIG technical testing

We also assessed CBP's SCRM plan for its HVA system. To comply with the most recent NIST SP 800-53 Rev. 5 controls, CBP must develop a system-level SCRM plan.[11] The SCRM plan should provide visibility and understanding of an entity's product development and integration, along with the processes used to ensure the system's integrity, security, resilience, and quality.

CBP did not develop a system-level SCRM plan because DHS delayed developing and publishing its department-level guidance instructing components to adopt

[11] According to NIST SP 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, September 2020, organizations are required to develop a plan for managing supply chain risks throughout the entire software development life cycle.

NIST SP 800-53 Rev. 5 controls, including system-level SCRM plans.[12]

During this review, CBP migrated its HVA from a server to a cloud-based environment as part of its modernization effort, which designated the HVA as a Federal Risk and Authorization Management Program (FedRAMP) system.[13] Cloud-based FedRAMP systems do not have a required date for implementing SCRM controls. As a result, we are not recommending that CBP develop and implement a system-level SCRM plan for its HVA. CBP has also retired the servers with configuration management deficiencies. Therefore, we did not recommend any corrective actions in that control family.

CBP Had an Effective Patch Management Process

CBP established an effective patch management process to remediate critical and high-risk vulnerabilities for the HVA databases we tested. CBP also had a remediation plan to ensure it applied all known software updates to the HVA databases, as required.[14] Our assessment of the HVA revealed four unique vulnerabilities (two critical and two high risk) related to server and computer weaknesses that occurred 208 times. Prior to our testing, CBP addressed all critical and high-risk vulnerabilities we identified by creating Plans of Action and Milestones, as required by DHS. Table 3 shows the results of our vulnerability assessment.

Table 3. Vulnerability Assessment Results

Operating System	Assets Scanned	Unique Critical Vulnerabilities	Unique High-Risk Vulnerabilities	Critical Vulnerability Instances	High-Risk Vulnerability Instances
Server Group One	11	0	0	0	0
Server Group Two	38	2	1	184	19
Database	5	0	1	0	5
Total	**54**	**2**	**2**	**184**	**24**

Source: DHS OIG technical testing

[12] In *Evaluation of DHS' Information Security Program for Fiscal Year 2021*, OIG-22-55, August 1, 2022, we recommended DHS revise DHS 4300A Policy, Handbook, and Ongoing Authorization methodology to incorporate applicable changes from NIST Special Publications, including SP 800-37, Revision 2, SP 800-53 Revision 5, and SP 800-137A, to maintain consistency among the documents. DHS concurred with the recommendation, which is resolved and closed.
[13] Established in 2011, FedRAMP standardizes Federal cybersecurity requirements for cloud services.
[14] DHS Policy Directive 4300A, *Information Technology System Security Program, Sensitive Systems (ITSSP SS)*, Version 13.3, February 13, 2023, requires that information security patches be installed in accordance with component plans, following the timeline for remediation published by the DHS Enterprise Security Operations Center.

Conclusion

CBP implemented most security and privacy controls we tested for the HVA and had an effective patch management process to remediate vulnerabilities in the HVA databases. Until FedRAMP systems are required to implement SCRM controls and DHS instructs components to adopt NIST SP 800-53 Rev. 5 controls, there is a risk that sensitive information stored and processed by HVA systems may not be fully protected and secure.

Objective, Scope, and Methodology

The Department of Homeland Security Office of Inspector General was established by the *Homeland Security Act of 2002* (Public Law 107–296), which amended the *Inspector General Act of 1978*.

The objective of our review was to determine whether CBP implemented effective technical controls to protect sensitive information on a selected HVA system. We focused our review on one CBP HVA system. To accomplish our objective, we determined whether CBP developed and implemented HVA system policies and procedures related to selected NIST control families. We specifically examined whether CBP had developed and implemented policies and procedures in the following areas:

- patch and configuration management;
- supply chain risk management;
- user account access management;
- audit trails;
- incident response;
- security awareness and role-based training;
- contingency planning; and
- data privacy protection.

We interviewed CBP officials and reviewed CBP's documentation and data for the HVA system to evaluate how the component implemented selected NIST SP 800-53 Revision 5 controls. We performed judgmental sampling in the areas of user account management, security awareness training, and role-based training. Internal specialists from DHS OIG's Office of Innovation, Cybersecurity Risk Assessment Division, conducted technical assessments to identify potential vulnerabilities, missing patches, and any noncompliance with applicable Defense Information Systems Agency Security Technical Implementation Guides configuration settings. To ensure the accuracy of testing results and OIG reporting, CBP reviewed our preliminary observations and identified "false-positive" results, as applicable. We reviewed CBP's feedback and updated our analysis as needed.

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 2022 and May 2023, under the authority of the *Inspector General Act of 1978*, 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.

The Office of Audit major contributors to this report were Chiu-Tong Tsang, Director, Information Technology Audits; Priscilla Cast, Audit Manager; Nathaniel Nicholson, Auditor-in-Charge; Gary Greer, Auditor; Brian Smythe, Auditor; Brendan Burke, Auditor; Lauren Barrick, Auditor; Omar Russell, Auditor; Lance Watkins, Auditor; Thomas Rohrback, Director, Cybersecurity Risk Assessment Division; Lawrence Polk, IT Cybersecurity Specialist; Jason Dominguez, IT Cybersecurity Specialist; Thomas Hamlin, Communications Analyst; and John Skrmetti, Independent Referencer.

DHS OIG Access to DHS Information

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

Appendix A
Summary of Other Control Family Testing Results

We focused our review on one CBP HVA system. To accomplish our objective, we tested CBP's technical controls and determined whether CBP developed and implemented HVA system policies and procedures related to the NIST control families. We found that CBP created a standard operating procedure that addressed all NIST access control family and DHS requirements. Specifically, CBP required that access agreements were:

- developed and documented;
- signed before individual system users gained access;
- re-signed, by all parties, when updated; and
- reviewed at least annually.

CBP maintained a current list of 30,272 HVA users and their authorized level of access, including three privileged users assigned to various groups. We selected judgmental samples of 53 HVA users — 50 non-privileged and all 3 privileged users, which included a mix of 43 CBP employees and 10 employees from various DHS components and non-DHS Federal agencies. Based on the supporting documents CBP provided, we determined all 53 HVA users sampled met access control, awareness training, and planning control family requirements. Specifically, sampled HVA users:

- were properly granted access to the system;
- received required security awareness training and role-based training;
- signed rules of behavior; and
- as applicable, were removed according to established procedures.

Separately, we judgmentally sampled 20 users from a universe of 1,219 and tested the removal process. We found that CBP removed access for all users who had retired, resigned, transferred, or been removed from positions requiring HVA system access. We concluded that CBP had an effective process to manage user account access upon employee and contractor separation.

CBP also implemented effective contingency planning for its HVA. We assessed CBP's plan and testing results in the system of record. CBP had the required contingency plans and conducted related testing, as required by the contingency planning control family. Both documents showed evidence of annual review, updates, and approval. Finally, the remaining three control families (incident response; audit and accountability; and assessment, authorization, and monitoring) were either inherited from CBP's enterprise level or had appropriate policies and procedures, as required.

Appendix B
NIST SP 800-53 Controls Reviewed Within Each Control Family

Control Family	Controls Tested	Deficiencies Identified	Controls Effective
(1) Configuration Management	Policy and Procedures	No	☑
	Configuration Settings	Yes	
(2) Risk Assessment	Privacy Impact Assessments	No	☑
	Vulnerability Assessments	No	
(3) Supply Chain Risk Management	Policy and Procedures	Yes	☒
	Supply Chain Risk Management Plan	Yes	
(4) Access Controls	Policy and Procedures	No	☑
	Account Management	No	
	Access Agreements	No	
(5) Planning	Policy and Procedures	No	☑
	Rules of Behavior	No	
(6) Awareness and Training	Policy and Procedures	No	☑
	Literacy Training and Awareness	No	
	Role Based Training	No	
(7) Assessment, Authorization, and Monitoring	Plan of Action and Milestones	No	☑
	Continuous Monitoring	No	
(8) Contingency Planning	Policy and Procedures	No	☑
	Contingency Plan	No	
	Contingency Plan Testing	No	
(9) Incident Response	Incident Reporting	No	☑
(10) Audit and Accountability	Policy and Procedures	No	☑
	Content of Audit Records	No	
	Audit Log Storage Capacity	No	
	Response to Audit Logging Failures	No	
	Audit Record Review, Analysis, and Reporting	No	
	Time Stamps	No	
	Audit Record Retention	No	

Source: DHS OIG analysis

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
CIO, CBP
Audit Liaison, CBP

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees

Additional Information and Copies

To view this and any of our other reports, please visit our website at: www.oig.dhs.gov.

For further information or questions, please contact Office of Inspector General Public Affairs at: DHS-OIG.OfficePublicAffairs@oig.dhs.gov.
Follow us on Twitter at: @dhsoig.

OIG Hotline

To report fraud, waste, or abuse, visit our website at www.oig.dhs.gov and click on the red "Hotline" box. If you cannot access our website, call our hotline at (800) 323-8603, or write to us at:

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