U.S. DEPARTMENT OF HOMELAND SECURITY

OFFICE OF INSPECTOR GENERAL

OIG-24-53 September 17, 2024

FINAL REPORT

ICE Did Not Fully Implement Effective Security Controls on Selected High Value Asset Systems

OFFICE OF INSPECTOR GENERAL

U.S. Department of Homeland Security

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

September 17, 2024

MEMORANDUM FOR: Patrick J. Lechleitner
Deputy Director and Senior Official Performing the Duties of the Director
U.S. Immigration and Customs Enforcement

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

JOSEPH V CUFFARI
Digitally signed by JOSEPH V CUFFARI
Date: 2024.09.17 19:08:19 -04'00'

SUBJECT: *ICE Did Not Fully Implement Effective Security Controls on Selected High Value Asset Systems*

Attached for your action is our final report, *ICE Did Not Fully Implement Effective Security Controls on Selected High Value Asset Systems*. We incorporated the formal comments provided by your office.

The report contains six recommendations aimed at improving security controls that protect sensitive information stored and processed on the selected ICE High Value Assets. Your office concurred with all six recommendations. Based on information provided in your response to the draft report, we consider recommendation 2 open and unresolved. As prescribed by Department of Homeland Security Directive 077-01, *Follow-Up and Resolutions for the Office of Inspector General Report Recommendations*, within 90 days of the date of this memorandum, please provide our office with a written response that includes your (1) agreement or disagreement, (2) corrective action plan, and (3) target completion date for the recommendation. Also, please include responsible parties and any other supporting documentation necessary to inform us about the current status of the recommendation. Until your response is received and evaluated, the recommendation will be considered open and unresolved.

We consider recommendations 1, 3, 4, 5, and 6 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 Kristen Bernard, Deputy Inspector General for Audits, at (202) 981-6000.

Attachment

DHS OIG HIGHLIGHTS

ICE Did Not Fully Implement Effective Security Controls on Selected High Value Asset Systems

September 17, 2024

Why We Did This Review

Across the Federal Government, various departments, including DHS, operate systems that contain sensitive information and support critical services. We performed this review to determine whether ICE has implemented security controls that protect sensitive information stored and processed on its selected HVAs.

What We Recommend

We made six recommendations to improve the security controls that protect sensitive information stored and processed on the selected ICE HVAs.

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

U.S. Immigration and Customs Enforcement (ICE) did not fully implement the necessary security controls to protect sensitive information processed by selected High Value Asset (HVA) systems. Specifically, ICE did not establish a cloud configuration standard or effectively monitor its HVAs' cloud security controls. This occurred because ICE's existing policy does not contain specific guidance for scanning the cloud-based platform for compliance with the Department of Homeland Security's configuration guidance.

Additionally, ICE security personnel did not always verify the results of vulnerability assessments they conducted on the HVAs we reviewed. We scanned one of the HVA systems and identified 60 instances of unsecure code related to 18 unique types of security-exploitable software weaknesses. This occurred because ICE has not implemented a monitoring process to ensure security personnel review and verify scan results. Finally, ICE did not fully document and review HVA system security baselines for accuracy in a timely manner because it did not have sufficient guidance or implement a process to ensure baseline reviews and updates were completed.

Potential consequences of the deficiencies we identified may include unauthorized access to confidential information and data manipulation or deletion. By not effectively monitoring its HVAs, ICE cannot be assured that the sensitive information stored and processed on these systems is protected and secure.

ICE Response

ICE concurred with all six recommendations. Appendix B contains ICE's management comments in their entirety.

Background

The U.S. Government continues to face increasingly sophisticated efforts to compromise Federal information technology systems — efforts that challenge current defenses and create an urgent need to evolve to a new security paradigm. 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 Office of Inspector General 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] Since 2015, the Federal Government's High Value Asset (HVA) initiative has focused on the protection of the Federal Government's most critical and high-impact information and information systems.[3] Across the Federal Government, agencies operate HVAs that contain sensitive information and/or support critical services. Agencies are principally responsible for designating their HVAs. An agency may designate Federal information or an information system as an HVA when it relates to one or more of the following categories:[4]

- **Informational Value** – The information or information system that processes, stores, or transmits the information is of high value to the Government or its adversaries.
- **Mission Essential** – The agency that owns the information or information system cannot accomplish its Primary Mission Essential Functions within expected timelines without the information or information system.
- **Federal Civilian Enterprise Essential** – The information or information system serves a critical function in maintaining the security and resilience of the Federal civilian enterprise.

The National Institute of Standards and Technology (NIST) developed guidance for categorizing and protecting Federal information and systems according to risk levels (High, Moderate, and Low). NIST Special Publication (SP) 800-53, Revision 4,[5] provides guidance on managing configurations to achieve more secure information systems within the Federal Government.

---

[1] *Department of Homeland Security's Annual Performance Report (APR) for FY 2021-2023*.
[2] Executive Order 14028, *Improving the Nation's Cybersecurity*, May 12, 2021.
[3] Cybersecurity and Infrastructure Security Agency Binding Operational Directive 18-02*, Securing High Value Assets,* May 7, 2018.
[4] Office of Management and Budget Memorandum 19-03, *Strengthening the Cybersecurity of Federal Agencies by enhancing the High Value Asset Program,* December 10, 2018.
[5] NIST SP 800-53, Revision 4*, Security and Privacy Controls for Information Systems and Organizations*, January 22, 2015. At the time of our automated compliance scans, ICE had not yet transitioned the FedRAMP ICE cloud-based platform to NIST 800-53, Revision 5.

Similarly, the *Federal Information Security Modernization Act of 2014*[6] requires each Federal agency to develop, document, and implement an enterprise-wide cybersecurity program to protect its systems and data.

U.S. Immigration and Customs Enforcement's (ICE) mission is to protect the United States by conducting criminal investigations and enforcing immigration laws to preserve national security and public safety. To accomplish its mission, ICE relies on its HVA systems to collect, process, and store large quantities of sensitive information. ICE has designated numerous systems as HVAs; most are hosted on a cloud-based platform that is also designated as an HVA. These systems serve various essential functions, such as capturing and storing records of healthcare services delivered to detainees in ICE custody.

We conducted this review to determine whether ICE has implemented security controls that protect sensitive information stored and processed on its selected HVAs. For this review, we randomly selected nine HVAs, including a cloud-based platform that hosts other systems. This report is one in a series of reviews on the effectiveness of IT security for various DHS component HVAs.

Results of Review

ICE Did Not Establish a Cloud Configuration Standard or Effectively Monitor Its HVAs' Cloud Security Controls

The Federal Government has developed several requirements for protecting Federal information and systems. DHS Directive 4300A[7] and NIST[8] require that specific configuration settings[9] be documented for information technology products implemented within the information system. DHS[10] also requires that components continuously monitor their systems to ensure compliance with security configuration guidance or best practices. As the operational lead for Federal cybersecurity, the Cybersecurity and Infrastructure Security Agency recommends that organizations use security tools to identify, detect, and mitigate cyber threats, vulnerabilities, and anomalies while operating in a hybrid or cloud environment.[11] The Office of Management

[6] Pub. L. No. 113-283, *Federal Information Security Modernization Act of 2014,* December 18, 2014.
[7] DHS Directive 4300A, *Information Technology System Security Program, Sensitive Systems,* Attachment CC, Rev4 ODP, February 13, 2023.
[8] Federal guidance provided a timeline for agencies to transition FedRAMP systems from NIST 800-53, Revision 4, to Revision 5. At the time of our automated compliance scans, ICE had not yet transitioned the FedRAMP ICE cloud-based platform to NIST 800-53, Revision 5.
[9] Configuration settings are the set of parameters that can be changed in an information system's hardware, software, or firmware components that affect the security posture and/or functionality of the system.
[10] DHS Directive 4300A, *Sensitive Systems Handbook*, Attachment O, *Vulnerability Management Program,* Version 15, May 2, 2019.
[11] Cybersecurity and Infrastructure Security Agency Factsheet, *Free Tools for Cloud Environments*, July 17, 2023.

and Budget[12] requires agencies to develop Plans of Action and Milestones to identify tasks that need to be accomplished to resolve information security weaknesses.

We found that ICE did not fully establish configuration settings for its cloud-based platform, which many HVAs reside on. The cloud platform's baseline did not specify the minimum-security configuration for the cloud environment. Instead, the system security baseline only identified configuration settings for web servers, operating systems, and databases. According to ICE security personnel, they had not designated a configuration baseline for the cloud-based platform because they are waiting for specific guidance from DHS' Office of the Chief Information Security Officer. DHS policy[13] allows components to use the Center for Internet Security (CIS) benchmarks[14] or recognized industry best practices,[15] which provide specific guidance that ICE needs for protecting its systems from cyberattacks. However, ICE did not develop its own guidance using industry best practices to protect its cloud-based platform.

DHS policy[16] also requires compliance verification through vulnerability assessments conducted at least monthly on all DHS systems and installation of vulnerability fixes according to the timeframe published by the Office of the Chief Information Security Officer. Although ICE did implement a continuous penetration testing program, ICE did not perform compliance scans of the cloud environment as required. Compliance scans are comprehensive examinations designed to ensure settings align with Department policy, whereas penetration testing focuses on specific vulnerabilities identified through reconnaissance tools and vulnerability scanners but is not sufficient to fully meet compliance requirements. This occurred because ICE did not have a configuration baseline to test against and ICE's *Vulnerability Scanning and Analysis Standard of Operation*[17] did not provide specific guidance on monitoring and scanning a cloud environment. Without baseline configuration settings and full scans of the cloud-based platform, ICE officials may not have appropriate visibility of security risks associated with the system and may miss opportunities to prevent data breaches or system disruption.

We initiated several automated compliance scans to assess the extent that ICE's cloud-based systems complied with CIS benchmarks and other industry standards. Our automated compliance scans identified 392 noncompliant security configuration settings on the ICE cloud platform. The noncompliant configuration settings we identified could result in unauthorized

[12] Office of Management and Budget Memorandum 02-01, *Guidance for Preparing and Submitting Security Plans of Action and Milestones*, October 17, 2001.
[13] DHS Directive 4300A, *Information Technology System Security Program, Sensitive Systems,* Attachment CC, Rev4 ODP, February 13, 2023.
[14] The Center for Internet Security is a community-driven nonprofit that is globally recognized for its best practices and benchmarks for securing information technology systems and data.
[15] Industry best practice security benchmarks focus on cloud-centric control areas. These controls are consistent with well-known security benchmarks, such as those described by CIS and NIST.
[16] DHS Directive 4300A, *Sensitive Systems Handbook*, Attachment O, Version 15, May 2, 2019.
[17] *Vulnerability Scanning and Analysis Standard of Operation,* Version 2, July 20, 2022.

access to confidential information and data manipulation or deletion. At the time of this report, ICE had initiated steps to address some of these weaknesses. Table 1 summarizes the results of our compliance scans.

Table 1. Results of DHS OIG Compliance Scans of ICE Cloud-Based Platform (July 13–20, 2023)

ICE Cloud-Based Platform[18]	Criteria	Total Unique Checks	Passed	Failed	Noncompliance Percentage
Service Provider #1	CIS Benchmarks	1,049	820	229	22%
Service Provider #2	CIS Benchmarks	175	136	39	22%
Service Provider #2	Industry Best Practice	364	240	124	34%

Source: DHS OIG audit team; based on the automated compliance scan results

ICE Security Personnel Did Not Always Verify the Results of Vulnerability Assessments

ICE's *Vulnerability Scanning and Analysis Standard of Operation*[19] requires ICE security personnel to verify all scan results to ensure that the scans were complete and credentialed (i.e., performed by someone who has proper authentication to access the system or database). A credentialed scan is more thorough than a non-credentialed (i.e., performed by someone without proper authentication) scan and provides a definitive list of required patches and misconfigurations. When verifying the results of web applications scans, ICE security personnel also need to search for indicators of an incomplete scan and/or insufficient credentials.

We reviewed the scan results ICE provided for seven HVAs for May and June 2023 and identified that 5 of the 16 scans[20] were non-credentialed. Although ICE security officials had identified three of the five non-credentialed scans and had taken corrective actions, they did not adequately verify the other two scan results to ensure they were credentialed scans, as required.

[18] ICE contracts with two vendors (known as cloud service providers) to support the cloud-based platform.
[19] *Vulnerability Scanning and Analysis Standard of Operation,* Version 2, July 20, 2022.
[20] Because one of the seven HVA systems had two operating systems, ICE conducted a total of eight vulnerability assessments for the HVA systems each month.

Additionally, we reviewed the web application scan results for one HVA for April through June 2023 and determined the three scans were incomplete. ICE security officials were not aware of the issue with these scans until we brought it to their attention.[21]

We performed our own automated web application scan[22] for the same HVA that had incomplete scans between April and June 2023. Our scan identified 60 instances of unsecure code[23] related to 18 unique types of security-exploitable software weaknesses. One type of high-risk vulnerability identified could enable an attacker to manipulate a website into divulging sensitive information. Table 2 depicts the results of our web application scan:

Table 2. DHS OIG Web Application Scan Results (August 3–17, 2023)

Vulnerabilities Based on Risk			
High	**Medium**	**Low**	**Total**
12	1	47	60

Source: DHS OIG–generated table; based on web application scan

ICE had not previously identified the vulnerabilities we found in our web application scan and did not have any plans or waivers for the identified software weaknesses. This occurred because ICE has not implemented a monitoring process to ensure that security personnel review and verify scan results. Without effective monitoring, insecure configurations and vulnerabilities may go undetected, thereby jeopardizing the protection and security of data within ICE's HVAs.

ICE Did Not Fully Document and Review Its HVA System Security Baselines for Accuracy in a Timely Manner

DHS Directive 4300A, Attachment CC, requires components to review and update each system security baseline[24] document at least annually. ICE's Process Bulletin-016 (the bulletin), *ICE System Baseline Template Guidance,*[25] requires the system security baseline to be properly

[21] During our assessment, we determined that ICE's resident scanning tool was not operating properly. ICE has since been in contact with the vendor to correct this issue.
[22] We were unable to use the same scanning tool ICE relied on to conduct its scans because the tool was inoperable; instead, we used another scanning tool provided by ICE to test the HVA against a configuration based on DHS criteria.
[23] Unsecured code is an example of a system flaw or weakness that originates from identifiable vulnerabilities in application programming. These vulnerabilities can be exploited to by an attacker to target the confidentiality, integrity, or availability of the system in question.
[24] Baseline security is defined as the minimum-security controls required for safeguarding an information technology system based on its identified needs for confidentiality, integrity, and/or availability protection.
[25] Security Assurance Branch, Process Bulletin-016, *ICE System Baseline Template Guidance (UPDATED),* October 27, 2021.

reviewed and approved monthly by multiple system security personnel (e.g., Information System Security Officer, Information Technology Program Manager, Administrator, Security Assurance Manager, and Information System Owner) and annually by the Chief Information Security Officer. The bulletin also requires that the system security baseline list all applicable configuration guides and additional baselines. These configurations guides and additional baselines serve as a basis for future builds, releases, or changes to systems and include security and privacy control implementations.

We reviewed the system security baselines for eight HVAs and found that seven of the eight baseline documents were approved annually. However, the baseline documentation for all HVAs did not contain evidence that monthly reviews and approvals occurred, as required. We also reviewed the listed configuration guides and additional baselines for the eight HVAs. Seven of the eight baseline documents either did not list the ICE cloud-based platform baseline or listed an out-of-date version.

These deficiencies occurred because ICE did not have sufficient guidance or implement a process to ensure its baseline review and updates were completed accurately and in a timely manner. The bulletin does not provide guidance on how to document the periodic review and approval of the system security baseline, or guidance on how to track the history of changes made to the baseline document. Also, ICE's baseline review and update process did not ensure that the system security baseline was reviewed and approved monthly or included all applicable benchmarks.

If system security baselines for ICE's HVAs are not regularly reviewed or do not accurately and completely document applicable configuration guides, ICE increases the risk that its systems will have noncompliant configurations. This, in turn, can enable malicious cyber actors to gain access to ICE's HVAs and compromise sensitive data in these systems.

Conclusion

Without accurate and up-to-date baselines and effective monitoring of its HVAs, ICE cannot be assured that the sensitive information processed by and stored on these systems is protected and secure. Furthermore, if cloud systems are not properly managed, ICE officials may not have appropriate visibility of security risks and may miss opportunities to prevent data breaches or system disruption.

Recommendations

Recommendation 1: We recommend the ICE Office of the Chief Information Officer, in coordination with DHS Office of the Chief Information Officer, establish and implement cloud

configuration standards for the selected High Value Asset systems in accordance with DHS configuration guidance.

Recommendation 2: We recommend the ICE Office of the Chief Information Officer develop and implement compliance scan guidance for the selected ICE cloud-based platform in accordance with applicable requirements.

Recommendation 3: We recommend the ICE Office of the Chief Information Officer ensure that the vulnerabilities identified in our assessments were remediated in a timely manner or that a Plans of Action and Milestones was created according to DHS and ICE policies.

Recommendation 4: We recommend the ICE Office of the Chief Information Officer develop a process to ensure scans for the selected High Value Assets are performed, reviewed, and verified according to applicable requirements.

Recommendation 5: We recommend the ICE Office of the Chief Information Officer update the security baseline policy with sufficient guidance to ensure the accurate review and approval of the system baseline documentation for the selected High Value Asset systems.

Recommendation 6: We recommend the ICE Office of the Chief Information Officer update and improve security baseline processes to ensure system baseline documentation is accurate and up to date for selected the High Value Asset systems.

Management Comments and OIG Analysis

ICE provided management comments on a draft of this report. We included the comments in their entirety in Appendix B. We did not receive any technical comments from ICE requiring revisions to the report. ICE concurred with all of six of our recommendations. We consider recommendation 1, 3, 4, 5, and 6 open and resolved, and recommendation 2 open and unresolved. A summary of ICE's response and our analysis follows.

ICE Comments to Recommendation 1: Concur. ICE's Office of the Chief Information Officer (OCIO) is currently ensuring that cloud configuration standards for HVA systems comply with DHS Policy Directive 4300A, which requires that specific configuration settings be enabled for IT products implemented within the information system. By December 31, 2024, ICE OCIO will duplicate these efforts to ensure that cloud service providers' CIS also complies with DHS configuration guidance. By March 31, 2025, ICE OCIO will correct identified weaknesses per NIST 800-53, Revision 5, and will implement "Policy as Code," a practice that allows organizations to use code to manage and automate the enforcement of policies for cloud cost optimization, security, compliance, and operations. Once "Policy as Code" is implemented, this new guidance

will improve the detection and remediation of vulnerabilities. Estimated Completion Date (ECD): May 30, 2025.

OIG Analysis of ICE Comments: ICE's actions are responsive to the recommendation. This recommendation will remain open and resolved until ICE provides documentation to support that all planned corrective actions are completed.

ICE Comments to Recommendation 2: Concur. ICE currently maintains procedures for vulnerability and compliance scanning, analysis, remediation planning, and Plans of Actions and Milestones management. For example, ICE's Cyber Defense and Intelligence Branch performs continuous penetration testing on ICE's cloud-based platform and all residing applications. These efforts will continue until the Application Support Branch Cloud Team has transitioned to "Policy as Code" by the end of March 2025, which will enforce compliance with requirements established by DHS Policy Directive 4300A. In April 2024, the ICE OCIO Cyber Risk Management and Assessment Branch implemented quality control testing to identify and correct procedural failures; corroborating documentation will be shared separately with DHS OIG. In addition, the ICE OCIO Cyber Risk Management and Assessment Branch is implementing enhanced training to ensure established Plans of Actions and Milestones management timelines are met. ECD: November 29, 2024.

OIG Analysis of ICE Comments: We agree ICE's penetration testing program plays an important role in identifying security vulnerabilities. However, compliance scans check configuration settings, whereas penetration tests narrowly focus on exploiting vulnerabilities found using reconnaissance tools and vulnerability scanners. Thus, compliance scan requirements established by DHS Policy Directive 4300A are not met by penetration tests. This recommendation will remain unresolved until ICE provides documentation that it has developed and implemented compliance scan guidance in accordance with the requirements set in DHS Policy Directive 4300A to ensure that monthly vulnerability assessments are performed on all systems.

ICE Comments to Recommendation 3: Concur. In October 2023, the ICE OCIO development and security teams for the selected HVA's system initiated a resolution process to address potential vulnerabilities with the web application and cloud configuration. Accordingly, 65 Plans of Actions and Milestones were established to address identified findings. As part of this process, ICE OCIO will ensure that cloud service provider's CIS also complies with DHS Directive 4300A. ECD: May 30, 2025.

OIG Analysis of ICE Comments: ICE's actions are responsive to the recommendation. This recommendation will remain open and resolved until ICE provides documentation to support that all planned corrective actions are completed.

ICE Comments to Recommendation 4: Concur. ICE OCIO adheres to DHS Directive 4300A regarding vulnerability scanning of all assets and applications within the ICE environment. For example, during October 2013, the ICE Vulnerability Assessment Team established processes and procedures for conducting operating system, database, and web application scans, as well as providing the results to the applicable stakeholders. The security team reviews and verifies the scan results before distributing them to stakeholders and opens Plans of Actions and Milestones to address any issues identified, as appropriate. In addition, the ICE OCIO Cyber Risk Management and Assessment Branch implemented quality control testing in April 2024 to identify and correct procedural deficiencies and will implement additional training to ensure established scanning procedures are followed. ECD: November 29, 2024.

OIG Analysis of ICE Comments: ICE's actions are responsive to the recommendation. This recommendation will remain open and resolved until ICE provides documentation to support that all planned corrective actions are completed.

ICE Comments to Recommendation 5: Concur. ICE OCIO HVA security teams follow ICE's Security Assurance Branch Process Bulletin 016, *System Baseline Update* (October 17, 2021), which outlines requirements for the review standard all ICE systems in step 2. Accordingly, ICE OCIO will review and update existing policies to ensure compliance with DHS Directive 4300A regarding approval of the system baseline documentation. ECD: November 29, 2024.

OIG Analysis of ICE Comments: ICE's actions are responsive to the recommendation. This recommendation will remain open and resolved until ICE provides documentation to support that all planned corrective actions are completed.

ICE Comments to Recommendation 6: Concur. ICE OCIO follows the Security Assurance Branch Process Bulletin 016, which addresses requirements for the review standard for all ICE systems. Accordingly, ICE OCIO will review and update system baseline procedures to ensure compliance with DHS Directive 4300A. In addition, ICE OCIO will develop updated training on security baseline development and management processes. ECD: November 29, 2024.

OIG Analysis of ICE Comments: ICE's actions are responsive to the recommendation. This recommendation will remain open and resolved until ICE provides documentation to support 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 review objective was to determine whether ICE has implemented security controls that protect sensitive information stored and processed on its selected HVAs. We received a list of all designated ICE HVA systems and judgmentally selected nine systems, including ICE's cloud-based platform, to review. To achieve our objective, we reviewed selected security controls relating to configuration and vulnerability management of the nine selected HVAs, all of which are part of ICE's information security program. We interviewed selected ICE officials to identify applicable DHS and ICE requirements for securing HVAs. We also reviewed ICE's security baseline documentation and vulnerability scan results for April through June 2023.

The team collaborated with internal specialists from DHS OIG's Office of Innovation, Cybersecurity Risk Assessment Division (CRA). CRA conducted technical assessments, using scanning tools, to identify potential vulnerabilities, and any configuration noncompliance with applicable CIS benchmarks and industry benchmarks. Additionally, CRA conducted a web application vulnerability assessment for a selected HVA using a commercially available scanning tool. To ensure that our test results and reporting were accurate, we gave ICE the opportunity to review our preliminary observations to identify "false-positive" results. We reviewed ICE'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 from June 2023 through March 2024 under the authority of the *Inspector General Act of 1978*, 5 United States Code §§ 401–424, and according to the *Quality Standards for Inspections and Evaluations*, issued by the Council of the Inspectors General on Integrity and Efficiency.

DHS OIG's Access to DHS Information

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

Appendix B:
ICE Comments on the Draft Report

Office of the Chief Financial Officer

U.S. Department of Homeland Security
500 12th Street, SW
Washington, D.C. 20536

U.S. Immigration and Customs Enforcement

BY ELECTRONIC SUBMISSION

July 31, 2024

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

FROM: Jennifer Cleary
JOHN T KIRSCH
Digitally signed by JOHN T KIRSCH
Date: 2024.07.31 11:35:30 -04'00'
Chief Financial Officer and
Senior Component Accountable Official
U.S. Immigration and Customs Enforcement

SUBJECT: Management Response to Draft Report: "ICE Did Not Fully Implement Effective Security Controls on Selected High Value Asset Systems" (Project No. 23-028-AUD-ICE)

Thank you for the opportunity to comment on this draft report. U.S. Immigration and Customs Enforcement (ICE) appreciates the work of the Office of Inspector General (OIG) in planning and conducting its review and issuing this report.

ICE leadership is pleased to note OIG's recognition that ICE utilizes high value asset (HVA) systems to collect, process, and store large quantities of sensitive information to serve essential functions as part preserving national security and public safety, such as capturing and storing healthcare services delivered to detainees in ICE custody. ICE remains committed to ensuring controls to safeguard sensitive information stored and processed on HVA systems.

The draft report contains six recommendations with which ICE concurs. Enclosed find our detailed response to each recommendation. ICE previously submitted technical comments addressing several accuracies, 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.

Enclosure

www.ice.gov

Enclosure: Management Response to Recommendations Contained in 23-028-AUD-ICE

OIG recommended the ICE Office of the Chief Information Officer (OCIO):

Recommendation 1: In coordination with DHS [the U.S. Department of Homeland Security] Office of the Chief Information Officer, establish and implement cloud configuration standards for the selected High Value Asset systems in accordance with DHS configuration guidance.

Response: Concur. ICE OCIO is currently ensuring that cloud configuration standards for HVA systems comply with DHS Policy Directive 4300A[1] which requires specific configuration settings be enabled for IT products implemented within the information system. By December 31, 2024, ICE OCIO will duplicate these efforts to ensure that Amazon Web Services Center for Internet Security (AWS CIS) also complies with DHS configuration guidance. By March 31, 2025, ICE OCIO will correct identified weaknesses in accordance with National Institute of Standards and Technology (NIST) 800-53 Rev 5[2], and will implement "Policy as Code," a practice which allows organizations to use code to manage and automate the enforcement of policies for cloud cost optimization, security, compliance, and operations. Once implemented, "Policy as Code", this new guidance will improve the detection and remediation of vulnerabilities. Estimated Completion Dates (ECD): May 30, 2025.

Recommendation 2: Develop and implement compliance scan guidance for the selected ICE cloud-based platform in accordance with applicable requirements.

Response: Concur. ICE currently maintains procedures for vulnerability and compliance scanning, analysis, remediation planning, and Plans of Actions and Milestones (POA&M) management. For example, ICE Cyber Defense & Intelligence Branch performs continuous penetration testing on the ICE Cloud Boundary Platform, and all residing applications. These efforts will continue until the Application Support Branch Cloud Team has transitioned to "Policy as Code" by the end of March 2025, which will enforce compliance with requirements established by DHS Policy Directive 4300A.

In April 2024, the ICE OCIO Cyber Risk Management and Assessment Branch implemented quality control testing to identify and correct procedural failures,

[1] "Information Technology System Security Program, Sensitive Systems," version 5, dated February 13, 2023.
[2] "Security and Privacy Controls for Information Systems and Organizations," dated September 2020; https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final

corroborating documentation of which will be shared separately with the OIG. In addition, the ICE OCIO Cyber Risk Management and Assessment Branch is implementing enhanced training to ensure established POA&M management timelines are met. ECD: November 29, 2024.

Recommendation 3: Ensure the vulnerabilities identified in our assessments are remediated in a timely manner, or a create a Plan of Action and Milestones as needed, according to DHS and ICE policies.

Response: Concur. In October 2023, the ICE OCIO Development and Security Teams initiated a resolution process to address potential vulnerabilities with the web application and cloud configuration. Accordingly, currently 65 POA&Ms were established to address identified findings. As part of this process, ICE OCIO will ensure that AWS CIS also complies with DHS Directive 4300A. ECD: May 30, 2025.

Recommendation 4: Develop a process to ensure scans for the selected High Value Assets are performed, reviewed, and verified according to applicable requirements.

Response: Concur. ICE OCIO adheres to DHS Directive 4300A with regard to vulnerability scanning of all assets and applications within the ICE environment. For example, during October 2013, the ICE Vulnerability Assessment Team established processes and procedures for conducting Operating System, Data Base and Web Application scans, as well as providing the results to the applicable stakeholders. The ICE Security Team reviews and verifies the scan results prior to distributing to stakeholders and opens POA&Ms to address any issues identified, as appropriate. In addition, ICE OCIO Cyber Risk Management and Assessment Branch implemented quality control testing in April 2024, to identify and correct procedural deficiencies, and will implement additional training to ensure established scanning procedures are followed. ECD: November 29, 2024.

Recommendation 5: Update the security baseline policy with sufficient guidance to ensure the accurate review and approval of the system baseline documentation for the selected High Value Asset systems.

Response: Concur. ICE OCIO HVA Security Teams follow Security Assurance Branch (SAB) "SAB Process Bulletin 016 – System Baseline Update," (October 17, 2021), which outlines requirements for review standard for all ICE systems in "step 2." Accordingly, ICE OCIO will review and update existing policies to ensure compliance with DHS Directive 4300 regarding approval of the system baseline documentation. ECD: November 29, 2024.

Recommendation 6: Update and improve security baseline processes to ensure system baseline documentation is accurate and up to date for the selected High Value Asset systems.

Response: Concur. ICE OCIO follow the SAB Process Bulletin 016, which addresses requirements for the review standard for all ICE systems. Accordingly, ICE OCIO will review and update system baseline procedures to ensure compliance with DHS Directive 4300A. In addition, ICE OCIO will develop updated training on security baseline development and management processes. ECD: November 29, 2024.

4

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, ICE
Audit Liaison, ICE

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