U.S. DEPARTMENT OF HOMELAND SECURITY

OFFICE OF INSPECTOR GENERAL

OIG-24-11

January 11, 2024

FINAL REPORT

Summary of Selected DHS Components That Did Not Consistently Restrict Access to Systems and Information

OFFICE OF INSPECTOR GENERAL
U.S. Department of Homeland Security
Washington, DC 20528 | www.oig.dhs.gov

January 11, 2024

MEMORANDUM FOR: Eric Hysen
Chief Information Officer
Department of Homeland Security

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

JOSEPH V CUFFARI
Digitally signed by JOSEPH V CUFFARI
Date: 2024.01.09 17:03:54 -07'00'

SUBJECT: *Summary of Selected DHS Components That Did Not Consistently Restrict Access to Systems and Information*

Attached for your action is our final report, *Summary of Selected DHS Components That Did Not Consistently Restrict Access to Systems and Information.* The Department of Homeland Security chose not to submit management comments. 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 DHS. 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

Summary of Selected DHS Components That Did Not Consistently Restrict Access to Systems and Information

January 11, 2024

Why We Did This Report

DHS components use IT access controls to help ensure only authorized users have access to systems and information. When properly implemented, access controls help prevent individuals from gaining inappropriate access to systems and data.

We issued this report to summarize the results of prior DHS Office of Inspector General audit reports pertaining to access control best practices and deficiencies, and the common issues that may warrant DHS' attention.

What We Recommend

The report summarizes previous recommendations and does not contain new recommendations.

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

Department of Homeland Security components did not consistently apply information technology (IT) access controls to ensure only authorized personnel had access to systems, networks, and information. This capping report summarizes access control practices and deficiencies reported in three components — U.S. Citizenship and Immigration Services (USCIS), Federal Emergency Management Agency (FEMA), and U.S. Immigration and Customs Enforcement (ICE) — over the last 12 months.

We determined USCIS, FEMA, and ICE did not consistently manage or remove access when personnel separated or changed positions. Also, USCIS, FEMA, and ICE did not take all necessary steps to ensure privileged user access was appropriate and that service accounts were adequately secured. These deficiencies stemmed from insufficient internal controls and oversight to ensure access controls were administered appropriately.

In addition to access control deficiencies, we found that USCIS, FEMA, and ICE did not implement all required security settings and updates for their IT systems. This occurred because the components were concerned these IT controls might negatively impact operations. We also found that DHS' information security framework did not include the latest Federal requirements for access controls. DHS' overall security posture relies on all components to implement effective IT access controls. Therefore, it is critical for USCIS, FEMA, and ICE to complete the corrective actions needed to fully address the deficiencies and the remaining 24 open recommendations made in our three prior reports.

Department Response

DHS chose not to submit management comments.

Table of Contents

Abbreviations

FEMA	Federal Emergency Management Agency
ICE	U.S. Immigration and Customs Enforcement
IT	information technology
USCIS	U.S. Citizenship and Immigration Services

Background

The Department of Homeland Security's critical mission of protecting the homeland makes its systems and networks high visibility targets for attackers who aim to disrupt essential operations or gain access to sensitive information.[1] One of the most effective ways to protect data and reduce the risk of a cyberattack is to enforce access controls by ensuring only appropriate users have access to an organization's network, systems, and information. Cyberattacks may come from external attackers who aim to breach cyber defenses and gain access to networks, programs, and applications or from insider threats (e.g., employees who use their authorized access to do harm).

All executive branch agencies must implement access controls as a part of their security framework to help protect their operations and assets from bad actors and other unauthorized users. In addition to using access controls, organizations can improve their ability to withstand cyberattacks by promptly addressing system vulnerabilities, using appropriate security settings, and keeping management informed about any security challenges. These efforts increase security awareness and minimize risks to systems by identifying, managing, and tracking security risks and threats until they are addressed.

During fiscal years 2022 and 2023, we issued three audit reports on the extent to which U.S. Citizenship and Immigration Services (USCIS),[2] Federal Emergency Management Agency (FEMA),[3] and U.S. Immigration and Customs Enforcement (ICE)[4] applied information technology (IT) access controls to permit appropriate access to systems and information. Each component collects sensitive information as part of its unique and critical mission to support DHS' overall efforts to secure the homeland. Specifically, this data collection includes the following:

- USCIS collects a significant amount of data, including biometric and personally identifiable information, to administer immigration benefits and requests for citizenship and lawful permanent residence, among other activities.

[1] DHS Management Directive 11042.1, *Safeguarding Sensitive But Unclassified Information*, January 6, 2005, defines sensitive security information as information obtained or developed in carrying out certain security or research and development activities to the extent that it has been determined that disclosure of the information would be an unwarranted invasion of personal privacy, reveal a trade secret or privileged or confidential commercial or financial information, or be detrimental to the safety of passengers in transportation.

[2] *USCIS Should Improve Controls to Restrict Unauthorized Access to Its Systems and Information*, OIG-22-65, September 7, 2022.

[3] *FEMA Should Improve Controls to Restrict Unauthorized Access to Its Systems and Information*, OIG-23-16, February 15, 2023.

[4] *ICE Should Improve Controls to Restrict Unauthorized Access to Its Systems and Information,* OIG-23-33, July 19, 2023.

- FEMA collects sensitive information from the public, including personally identifiable information and financial data, to provide disaster support.
- ICE investigates transnational crimes and threats, specifically those from criminal organizations that seek to exploit the global infrastructure through which international trade, travel, and finance move. ICE collects large amounts of data to support its critical law enforcement mission.

The objective of this report is to summarize the results of prior DHS Office of Inspector General audit reports pertaining to access control best practices and deficiencies, as well as the common issues that may warrant DHS' attention.

Results of Capping Report

DHS components did not consistently apply the IT access controls needed to restrict unnecessary access to their systems, networks, and information. This capping report provides a summary of access control deficiencies and 27 recommendations found in our three audit reports[5] issued in the last 12 months that require DHS management's attention.

We determined USCIS, FEMA, and ICE had similar access control deficiencies and challenges restricting unnecessary IT access. These deficiencies stemmed from insufficient internal controls and oversight to ensure access controls were administered appropriately. In addition to access control deficiencies, we found all three components did not implement required security settings and updates for their IT systems. This occurred because the components were concerned these IT controls might negatively impact operations. We also found DHS' information security framework did not include the latest Federal requirements for access controls because of an inconsistent process for identifying and implementing required policy changes. DHS' overall security posture requires all components implement effective IT access controls. Therefore, it is critical for USCIS, FEMA, and ICE to complete the corrective actions needed to fully address the deficiencies and 24 open recommendations made in our three prior reports.

DHS Components Did Not Effectively Manage Access to Systems and Information

Although USCIS, FEMA, and ICE implemented access control requirements for their systems, the components did not consistently manage or remove access for personnel who separated or changed positions. Additionally, the components did not meet requirements for monitoring and assigning privileged user access and for securing service accounts. We attributed these deficiencies to insufficient internal controls and oversight to ensure access controls were administered appropriately and effectively to prevent unauthorized access.

[5] See OIG-22-65, OIG-23-16, and OIG-23-33.

DHS Components Did Not Appropriately Remove Access for Separated and Transferred Personnel

Removing system access for separated and transferred personnel is an effective method for preventing individuals who no longer have a mission need to access information. DHS requires[6] system access to be removed or updated appropriately when an individual separates or transfers positions. However, USCIS, FEMA, and ICE did not consistently manage or remove access for personnel who separated or transferred positions.

Even though DHS policy requires that access for separated personnel must be disabled immediately, we found that, on average, 64 percent of separated individuals we tested had access to DHS systems and information beyond their last workday. Table 1 lists the total number and percentage of USCIS, FEMA, and ICE personnel who separated and did not have their access removed in a timely manner.

Table 1. Separated Personnel Who Had Unnecessary Access to Information

Findings	USCIS	FEMA	ICE	Total
Total of Separated Personnel Accounts Not Removed Timely	98	263	159	520
Percent of Noncompliant Separated Personnel Accounts	33%	75%	84%	--

Source: DHS OIG analysis of access control findings

We determined USCIS, FEMA, and ICE did not remove access for separated personnel in a timely manner because supervisors did not appropriately follow component account deactivation procedures. USCIS and ICE supervisors were required[7] to submit account deactivation requests

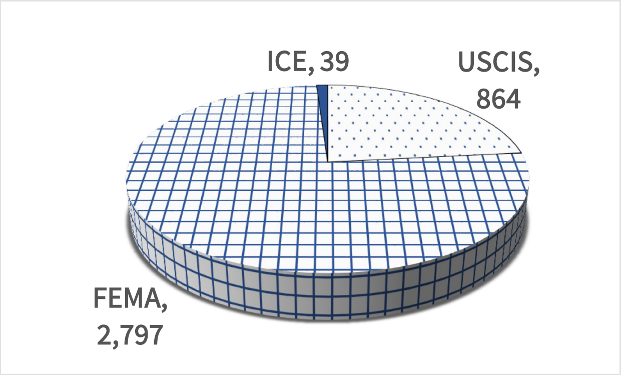
[6] *DHS Sensitive Systems Policy Directive 4300A*, Version 13.1, July 27, 2017, provided the requirements we used for the prior audits this capping report is based on. DHS published a revised policy directive, DHS 4300A, *Information Technology Systems Security Program, Sensitive Systems*, Version 13.2, on September 20, 2022.

[7] *USCIS Account Management Directive*, 140-006.1, July 10, 2017, and *ICE OCIO IRMnet Account Management Procedure*, October 15, 2019.

for access removal, but they did not always promptly complete these requests. Similarly, FEMA supervisors were required[8] to schedule account access to be removed before separated personnel's last workday, but supervisors did not consistently follow this process. Further, we noted that although supervisors at USCIS, FEMA, and ICE did not follow prescribed account deactivation processes, all three components implemented automated backup controls to remove access if supervisors did not take action to remove account access as required. USCIS implemented controls to remove access after 30 days of inactivity, and ICE had a similar process with removal at 45 days. FEMA used automated controls to remove system access if an employee's pay status changed in the National Finance Center database, or their personal identity verification card became inactive.

In addition to not removing access for separated personnel, USCIS, FEMA, and ICE did not have a process to ensure appropriate access privileges were assigned for individuals that transferred within their components. During our audits, components did not provide evidence that they had reviewed system access or removed unneeded privileges for 3,700 individuals who transferred positions within USCIS, FEMA, and ICE (Figure 1).

Figure 1. Unmonitored Transferred Personnel Across Components



Source: DHS OIG analysis of prior access control findings

USCIS, FEMA, and ICE did not review access for individuals who transferred offices because they did not have processes to identify and enforce access changes required when an individual moved within the component to a new position. Instead of formally tracking and enforcing access control requirements, each component expected personnel, such as supervisors and application gatekeepers,[9] to proactively identify transferred personnel whose access needed to be reviewed.

[8] *FEMA Accounts Management Standard Operating Procedure*, April 3, 2020.
[9] Application gatekeepers are personnel who help system owners manage access controls.

Components' Plans to Improve Access Controls for Separated and Transferred Personnel

To address these deficiencies, we recommended that all three components develop and implement additional processes to help ensure they remove access for separated and transferred personnel in a timely manner. All three components concurred with our recommendations and are taking steps to address deficiencies. To improve controls over removing separated personnel's access, USCIS and ICE plan to develop automated capabilities that improve their processes for identifying and removing access for separated personnel, and FEMA committed to increasing training and coordination for its access management processes.

Further, due to each component not having a formalized process to track and enforce access control requirements for transferred personnel, we recommended USCIS, FEMA, and ICE implement processes to identify and verify transferred personnel's access. In response to our recommendations, all three components are taking steps to implement additional internal controls to manage transferred personnel's access. For example, ICE will implement an access lifecycle management solution that provides automated capabilities for identifying transferred personnel, while USCIS and FEMA plan to develop processes to increase coordination and tracking of transferred personnel. A full list of the recommendations we have made to USCIS, FEMA, and ICE can be found in Appendix B.

Components Did Not Adequately Monitor and Assign Privileged User Access

Privileged users who are trusted to perform critical IT security functions may be granted powerful (i.e., high-level) access to sensitive assets. Attackers often covet privileged accounts because of the broad access typically granted to them. We found that although all three components had criteria for monitoring privileged user accounts, USCIS and FEMA did not monitor these accounts as required. During our audits, we identified 1,572 privileged user accounts that were not in compliance with requirements to periodically review account privileges, which included 599 USCIS and 973 FEMA accounts.

We also found both USCIS and FEMA were unable to monitor privileged user accounts because of inadequate processes. USCIS used an access management system to administer and monitor access, but the system did not provide the capability to monitor privileged accounts. FEMA relied on individual system owners to develop their own manual processes. However, system owners inconsistently applied these processes.

Additionally, DHS requires that account access be restricted to only those users with a mission need.[10] However, USCIS, FEMA, and ICE did not always appropriately restrict access to privileged

[10] *DHS Sensitive Systems Policy Directive 4300A*, Version 13.1, July 27, 2017, provided the requirements we used for the prior audits forming the basis of this capping report. DHS published a revised policy directive, DHS 4300A, *Information Technology Systems Security Program, Sensitive Systems*, Version 13.2, on September 20, 2022.

accounts. We found that all three components unnecessarily granted individuals access to sensitive privileged accounts even though this access was not required for their positions. In fact, across all three components, we identified 436 users who held inappropriate access to privileged accounts and may have had access to sensitive assets (Table 2).

Table 2. Users Found with Unnecessary Privileged Access

USCIS	FEMA	ICE	Total
61	259	116	436

Source: DHS OIG analysis of prior access control findings

Across all components, these inappropriate privileges were granted by mistake. Components explained that permissions were inherited indirectly through another permission that was approved for the accounts.

DHS' Efforts to Improve Privileged User Access Management

We recommended USCIS and FEMA develop and implement a process that allows for improved monitoring of privileged account access. Both components were responsive to our recommendations, as they agreed to either enhance access management system capabilities or to implement additional manual controls that allow for increased monitoring of privileged user access.

To address the permissions that were granted in error, we recommended that all three components take the necessary steps to ensure appropriate privileges. All three components concurred with our recommendations, and they agreed to evaluate the affected accounts and remove the inappropriate privileges as needed.

Service Accounts Were Not Secured from Potential Compromise

Components use service accounts to help execute automated tasks, such as running system commands or exchanging data with other systems. Service accounts pose unique security risks because they are non-human accounts and may have highly privileged access. Accordingly, DHS requires that service account passwords be changed at least annually and that all service accounts be appropriately encrypted[11] to reduce the risk of unauthorized access.

[11] Change Memorandum 13.1.1. to *DHS Sensitive Systems Policy Directive 4300A*, October 2, 2019, provided the requirements we used for the prior audits forming the basis of this capping report. This memorandum was also superseded by DHS 4300A, *Information Technology Systems Security Program*, *Sensitive Systems*, Version 13.2.

We found USCIS, FEMA, and ICE did not adequately manage service account passwords. During our audits, we identified 2,656 service accounts across the three components that did not follow DHS password guidance. USCIS had not changed the passwords for 653 service accounts within the past year, while FEMA and ICE configured service account passwords to not expire for 1,454 and 549 accounts, respectively.

Although each component had its own unique cause for not meeting service account password requirements, all three components faced underlying challenges associated with ineffective service account management. USCIS used service accounts that required manual password changes, and thus it could not manage security settings appropriately. FEMA used a manual system to monitor expiring service account passwords, and it did not enforce requirements. ICE did not have a process to review service account passwords because its internal policy contradicted DHS guidance during the time of our audit.

We determined that, in addition to not meeting service account password requirements, FEMA and ICE did not adequately meet encryption requirements for 48 and 816 service accounts, respectively. FEMA and ICE service accounts were not appropriately encrypted because the components were concerned that encryption would negatively impact system operations. Specifically, FEMA believed DHS' required level of encryption could negatively affect operations for its legacy IT assets. Similarly, ICE officials stated that previous attempts to implement required encryption standards had negatively affected applications and operations.

USCIS, FEMA, and ICE Are Taking Steps to Address Service Account Deficiencies

To address the password deficiencies, we recommended all three components implement automated tools or additional controls to help ensure service account passwords are changed as required. In response to our recommendations, all three components agreed to take corrective actions to address service account password deficiencies. FEMA and ICE plan to implement additional automated controls for tracking and updating service account passwords, as required, while USCIS plans to review all service accounts and update passwords to ensure DHS requirements are met.

We recommended that FEMA evaluate whether encryption could be implemented on affected service accounts. We also recommended that both FEMA and ICE submit waiver or risk acceptance requests to the DHS Chief Information Security Officer if technical limitations prevent required encryption settings from being applied. Both components concurred with our recommendations and agreed to further evaluate the affected accounts to determine if encryption settings could be applied.

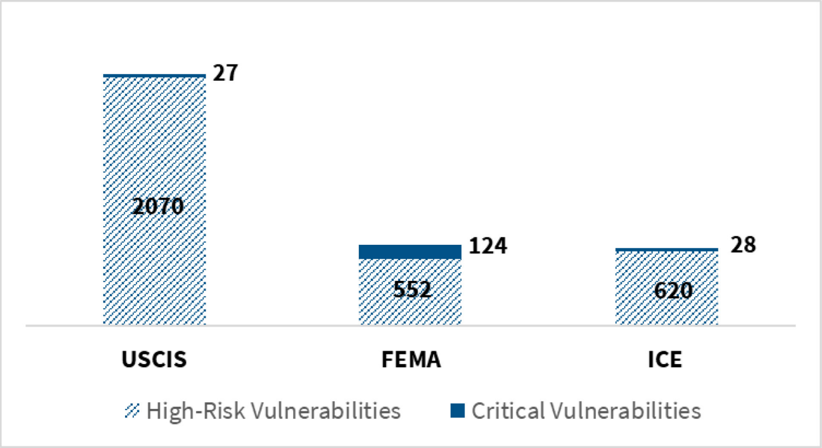
DHS Components Did Not Implement Required Settings and Address IT Infrastructure and Workstation Vulnerabilities

DHS components must address IT infrastructure and workstation vulnerabilities in their systems by installing timely system updates to minimize security risks. Additionally, DHS components rely on systems being configured with the appropriate settings to reduce potential security risks. Based on the analysis conducted during each audit, USCIS, FEMA, and ICE did not implement all required updates and security settings for their IT systems and workstations to help reduce the impact if access control weaknesses are exploited.

DHS Components Did Not Implement Required Updates to Address Vulnerabilities

USCIS, FEMA, and ICE did not remediate all critical and high-risk vulnerabilities within DHS' required timelines. The scans conducted during each audit identified critical and high-risk vulnerability occurrences that required remediation (Figure 2).

Figure 2. Critical and High-Risk Vulnerabilities Identified in Components' Systems



Source: DHS OIG analysis of prior access control findings

Overall, the components each explained how they faced operational challenges that prevented vulnerabilities from being addressed in a timely manner. For example, USCIS faced technical issues with its vulnerability management process, while FEMA and ICE explained the complexity of their IT operations posed challenges for implementing required system updates. Without implementing corrective patches to fix vulnerabilities identified in our testing, components risk access control weakness exploitation, as well as reduced confidentiality, integrity, and availability of sensitive systems and information.

DHS Components Did Not Implement Required Security Settings

DHS components must use system security settings that are consistent with technical frameworks, including the Defense Information Systems Agency's *Security Technical Implementation Guides*. However, USCIS, FEMA, and ICE did not fully implement all required settings for the systems we tested. We identified system security setting compliance rates as high as 98 percent[12] and as low as 58 percent.[13] All three components believed if they fully implemented the required settings set forth by the Defense Information Systems Agency's *Security Technical Implementation Guides,* these settings would have negatively affected their operations, thereby disrupting their ability to achieve their missions.

DHS' Efforts to Update System Settings and Address Known Vulnerabilities

We recommended all three components implement additional procedures or identify automated tools to help address known vulnerabilities within required timeframes. All three components were responsive to our recommendations and will evaluate their current vulnerability management programs, implementing new processes and automation where possible.

Additionally, we recommended USCIS implement all required settings or request a waiver from the DHS Chief Information Security Officer for settings it could not implement. Due to the unique nature of FEMA's process for managing system security settings,[14] we recommended FEMA work with the DHS Chief Information Security Officer to verify its process complied with DHS waiver and risk-acceptance requirements and for the DHS Chief Information Security Officer to evaluate FEMA's compliance with Federal Information Security Modernization Act scorecard requirements. FEMA and the DHS Chief Information Security Officer concurred with our recommendations. FEMA plans to complete a review of its standard operating procedures and submit the results of their analysis to the DHS Chief Information Security officer for verification of compliance. Additionally, the DHS Chief Information Security Officer completed corrective action by evaluating a review of FEMA's Federal Information Security Modernization Act scorecard submissions and confirmed FEMA complied with applicable requirements. We did not issue a recommendation to ICE because it formally created plans during our audit testing to address noncompliant settings in FY 2023.

DHS Had Not Updated Its Guidance for Access Controls

DHS' overall security posture relies on components implementing effective IT security processes. Therefore, DHS developed *DHS Sensitive Systems Policy Directive 4300A* to provide direction to

[12] We identified one USCIS system with this compliance rate.

[13] We identified one USCIS system and one FEMA system with this compliance rate.

[14] FEMA developed a component-specific process through its *Enterprise Compliance Baselines Standard Operating Procedure* to determine whether specific settings could be implemented rather than seek DHS-level approval.

managers and senior leadership on how to manage and protect sensitive systems. All DHS components, including USCIS, FEMA, and ICE, rely on this departmental guidance. We found the Policy Directive 4300A did not include the latest Federal requirements for access controls. We identified at least 88 access control changes or additions that were included in the latest Federal requirements[15] that were not addressed in DHS' guidance. DHS did not update its guidance due to the absence of a standardized change management process for identifying and implementing required changes.

DHS Has Taken Corrective Actions to Update Its Guidance

We recommended the DHS Chief Information Officer update Policy Directive 4300A with the latest Federal requirements and develop a formalized change management process for future updates. The DHS Chief Information Officer was responsive to our recommendations and, in September 2022, published DHS 4300A, *Information Technology Systems Security Program, Sensitive Systems,* to help ensure consistency with the latest Federal guidance. The DHS Chief Information Officer also formalized the change management process for future policy updates that it may need to include in its cybersecurity policy. Based on the DHS Chief Information Officer's corrective actions, we closed the two recommendations that were made to address IT policy deficiencies.

Conclusion

DHS components' access control deficiencies increase the risk that unauthorized individuals could access sensitive information or disrupt mission operations. Based on the conditions outlined in this report, USCIS, FEMA, and ICE access control and system security deficiencies may limit the Department's ability to reduce the risk of unauthorized access to its network and data. These deficiencies may also hinder DHS in efforts to mitigate the impact to operations if access control weaknesses are exploited. Although DHS and its components have begun taking steps to address our prior recommendations, it is critical for the Department to complete the corrective actions included in our 24 open recommendations to fully address the deficiencies in its operations.

Management Comments and OIG Analysis

DHS chose not to submit management comments.

[15] We found that DHS guidance did not include updates made by the National Institute of Standards and Technology in its Special Publication 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, September 2020.

Appendix A: 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) by amendment to the *Inspector General Act of 1978*.

Our objective was to summarize the results of prior DHS OIG reports pertaining to access control best practices and deficiencies, and the common issues that may warrant DHS' attention. The scope of this audit included results from audits we previously conducted[16] to determine the extent to which USCIS, FEMA, and ICE applied IT access controls to restrict unnecessary access to systems and information. To accomplish our objective, we examined the audit findings and conclusions of the three audit reports within the scope of this audit. We analyzed the findings, root causes, and recommendations from the reports to identify common themes and unique findings across USCIS, FEMA, and ICE.

We conducted work for this report between May and July 2023 pursuant to the *Inspector General Act of 1978*, 5 U.S.C. §§ 401–424. This capping report summarizes the key findings of audits that were conducted according to generally accepted government auditing standards.

DHS OIG's Access to DHS Information

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

[16] See OIG-22-65, OIG-23-16, and OIG-23-33.

Appendix B:
Summary of Previous Recommendations Issued to DHS

DHS Component	Recommendation	Estimated Completion Date
DHS Chief Information Officer	We recommend the DHS Chief Information Officer update the DHS 4300A Policy Directive and Handbook with the access control updates required by National Institute of Standards and Technology 800-53, Revision 5.	Closed
	We recommend the DHS Chief Information Officer develop a formalized change management process to identify and implement 4300A policy updates as governing policies and standards require.	Closed
	We recommend the DHS Chief Information Security Officer finalize its evaluation of FEMA's compliance with DHS' Federal Information Security Modernization Act Scorecard requirements and ensure any necessary remedial action.	Closed
USCIS	We recommend the Office of Human Capital and Training in conjunction with the Office of Information Technology evaluate the Employee and Contractor Exit Clearance Process and update as needed to ensure it provides the controls necessary to identify and communicate all separated employees in accordance with DHS policy of immediately revoking access to network and systems.	February 2024
	We recommend the Office of Human Capital and Training in conjunction with the Office of Information Technology develop and implement a process to identify all transferred employees and ensure that their access is reviewed and verified immediately in accordance with DHS policy.	February 2024
	We recommend the Office of Information Technology develop and implement a myAccess capability or an alternative manual review process to ensure that all privileged user and service account accesses are reviewed and validated at least annually.	February 2024
	We recommend the Office of Information Technology finalize the implementation of the proposed tiered privileged account project that allows users to use separate accounts when accessing less secure assets.	February 2024
	We recommend the Office of Information Technology implement managed service accounts or additional manual/technical controls to deny interactive logon and reset service account passwords timely.	February 2024
	We recommend the Office of Information Technology perform an evaluation of Active Directory configurations based on users' roles and responsibilities and remove unnecessary privileges that allow access to service accounts.	February 2024

DHS Component	Recommendation	Estimated Completion Date
	We recommend the Office of Information Technology finalize and implement patching procedures for assessing and resolving system vulnerabilities.	March 2026
	We recommend the Office of Information Technology implement all required Defense Information Security Agency's *Security Technical Implementation Guides* configuration settings for Enterprise Hosting Services, Enterprise Infrastructure Services, and Identity Credential Access.	March 2026
FEMA	We recommend the FEMA Chief Security Officer provide training to supervisors, contracting officer's representatives, contracting officers, human resource liaisons, and timekeepers on FEMA's offboarding processes for removing IT access.	September 2023
	We recommend the FEMA Chief Security Officer develop and implement internal controls to monitor and enforce supervisors and contracting officer's representatives' compliance with the Access Lifecycle Management system's offboarding process for removing IT access.	March 2024
	We recommend the FEMA Chief Security Officer implement a process to identify and verify that transferred personnel's unneeded access is removed in accordance with FEMA requirements.	March 2024
	We recommend the FEMA Office of the Chief Information Officer implement a standardized process to conduct and monitor privileged and service account reviews in accordance with FEMA requirements.	April 2025
	We recommend the FEMA Office of the Chief Information Officer remove the unnecessary privileges that allowed additional users to access the sensitive security account we identified.	April 2025
	We recommend the FEMA Office of the Chief Information Officer implement automated tools or additional controls and policies to change service account passwords as required and prevent interactive logon.	April 2025
	We recommend the FEMA Office of the Chief Information Officer establish a risk-based approach to implement DHS' required encryption standards where possible or submit requests for waivers or risk acceptance to the DHS Chief Information Security Officer to forgo this setting on affected FEMA service accounts.	January 2024
	We recommend the FEMA Office of the Chief Information Officer submit its FEMA *Enterprise Compliance Baselines Standard Operating Procedure* to the DHS Chief Information Security Officer to verify FEMA's compliance with DHS' waiver and risk acceptance requirements for Defense Information Security Agency's *Security Technical Implementation Guides* settings that are not implemented.	August 2023

DHS Component	Recommendation	Estimated Completion Date
	We recommend the FEMA Office of the Chief Information Officer perform an evaluation to identify additional automated tools to help address known vulnerabilities within required timeframes and implement where possible or formally accept the risk in accordance with DHS requirements.	January 2024
ICE	We recommend the ICE Office of the Chief Information Officer develop and implement processes to remove separated employees' access to all ICE systems, networks, and applications in accordance with DHS policy.	June 2024
	We recommend the ICE Office of the Chief Information Officer develop and implement a process to identify all transferred employees and ensure their user group access is reviewed and verified immediately at the end of their prior position in accordance with DHS policy.	June 2024
	We recommend the ICE Office of the Chief Information Officer develop and implement a repeatable process to conduct and monitor privileged user and service account reviews in accordance with DHS policy.	June 2024
	We recommend the ICE Office of the Chief Information Officer remove the unnecessary privileges that allow additional users to access the sensitive security account we identified.	January 2024
	We recommend the ICE Office of the Chief Information Officer submit requests for waivers or risk acceptance to the DHS Chief Information Security Officer to forgo implementing DHS' required encryption setting on affected ICE service accounts.	November 2023
	We recommend the ICE Office of the Chief Information Officer develop and implement measures to ensure service account passwords are updated as required.	June 2024
	We recommend the ICE Office of the Chief Information Officer evaluate its vulnerability management program to identify and implement automated tools to help address known vulnerabilities within required timeframes.	March 2024

Source: DHS OIG summary of prior report recommendations

Appendix C: Office of Audits Major Contributors to This Report

Tarsha Cary, Director
Alexander Stewart, Audit Manager
Kenneth Schoonover, Auditor-in-Charge
Alexandria Castaneda, Auditor
Tessa Clement, Auditor
Mark Lonetto, Independent Referencer
Tom Hamlin, Communications Analyst

Appendix D:
Report Distribution

Department of Homeland Security

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

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