OFFICE OF INSPECTOR GENERAL

ICE Should Improve Controls to Restrict Unauthorized Access to Its Systems and Information

Homeland Security

July 19, 2023

OIG-23-33

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

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

July 19, 2023

MEMORANDUM FOR: Patrick J. Lechleitner
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: 2023.07.18 17:34:18 -04'00'

SUBJECT: *ICE Should Improve Controls to Restrict Unauthorized Access to Its Systems and Information*

Attached for your action is our final report, *ICE Should Improve Controls to Restrict Unauthorized Access to Its Systems and Information.* We incorporated the formal comments provided by your office.

The report contains seven recommendations aimed at improving U.S. Immigration and Customs Enforcement (ICE) access controls. Your office concurred with all seven recommendations. Based on information provided in your response to the draft report, we consider all 7 recommendations 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. 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 call 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

ICE Should Improve Controls to Restrict Unauthorized Access to Its Systems and Information

July 19, 2023

Why We Did This Audit

ICE uses IT access controls to help ensure only authorized users have access to its systems and information. When properly implemented, access controls help to prevent individuals from gaining inappropriate access to systems or data. Our audit objective was to determine the extent to which ICE applied IT access controls to restrict unnecessary access to systems and information.

What We Recommend

We made seven recommendations to improve ICE's IT access controls and system security.

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 consistently implement effective access controls to restrict access to its network and information technology (IT) systems. Although ICE took a multi-layered approach to managing access for personnel who change positions or leave the component altogether, we determined that ICE did not consistently manage or remove access when personnel separated or changed positions. For example, 84 percent of the accounts for separated personnel we examined remained active beyond the individual's last workday. Additionally, ICE did not monitor and configure privileged user access, service accounts, and access to sensitive security functions as required. These deficiencies stemmed from insufficient internal controls and oversight of user account management and compliance to ensure access controls were administered appropriately and effectively to prevent unauthorized access.

Based on our testing, ICE did not implement all security settings for its IT systems and workstations because it was concerned that these settings negatively impacted system operations. In addition, according to officials, ICE accepted the risk of not implementing the required settings but did not provide any supporting evidence.

The deficiencies identified during this audit exposed ICE's network and IT systems to risks of compromise by potential attackers. ICE is taking steps to enhance its access control processes. However, until these deficiencies are addressed ICE's network and IT systems remain at risk. Additionally, these deficiencies could have limited the Department's overall ability to reduce the risk of unauthorized access to its network, which may disrupt mission operations.

ICE Response

ICE concurred with all seven recommendations. We have included a copy of ICE's comments in Appendix B.

Table of Contents

Appendixes

Abbreviations

ALM	Account Lifecycle Management
DISA	Defense Information Security Agency
ECD	Estimated Completion Date
FEMA	Federal Emergency Management Agency
GMSA	group managed service accounts
ICE	U.S. Immigration and Customs Enforcement
IT	information technology
OCIO	Office of the Chief Information Officer
PAM	Privileged Access Manager
PLAnet	Principal Legal Advisor Network
STIG	Security Technical Implementation Guide
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. For example, senior DHS officials' email accounts were compromised during the 2020 SolarWinds incident. During this cyberattack,[1] external attackers breached cyber defenses to gain access to Federal Government networks.[2] Once inside the networks, the attackers successfully set up permissions for themselves to access other programs and applications while being undetected.[3]

The Cybersecurity and Infrastructure Security Agency revealed that external attackers had gained access to a Federal agency's network in February 2022 by exploiting a vulnerability that had been well known since December 2020.[4] In this case, hackers moved throughout the agency's network, compromised credentials, and then maintained access to the agency to mine cryptocurrency on a U.S. Government network. Attacks can also come from within an organization — insider threats (i.e., employees or contractors who use their authorized access to do harm) pose additional cybersecurity risks.

Access controls ensure that only authorized users have job-related access to an organization's networks, systems, and computer accounts. Accordingly, U.S. Immigration and Customs Enforcement (ICE) implemented Microsoft Active Directory, which enables administrators to manage permissions and access to network resources (i.e., files, printers, database servers, and accounts) to allow users to accomplish their assigned duties. Active Directory provides the primary apparatus for authenticating users and determining which network resources they can access. Active Directory contains a list of all objects (i.e., a single element such as a network user, computer account, server, and printer) within the domain. It also keeps access control lists of the resources or objects a user has access to within the domain and verifies that access when a user tries to access an object or resources.

[1] *Remediating Networks Affected by the SolarWinds and Active Directory/M365 Compromise*, May 14, 2021.

[2] *Written Testimony of Sudhakar Ramakrishna, Chief Executive Office, SolarWinds, Inc.*, United States Senate Select Committee on Intelligence, February 23, 2021, and *SolarWinds hack got emails of DHS head and other top officials,* The Associated Press, March 29, 2021.

[3] *The SolarWinds Hackers Used Tactics Other Groups Will Copy*, January 19, 2021.

[4] *Iranian Government-Sponsored APT Actors Compromise Federal Network, Deploy Crypto Miner, Credential Harvester*, November 25, 2022.

All executive branch agencies must implement access controls[5] as part of their security framework to protect their operations and assets from being compromised by bad actors and other unauthorized users. Table 1 lists established access controls best practices for DHS personnel based on DHS criteria.

Table 1. Overview of Access Control Phases

Access Control	Control Description
Initial Approval of Access	Individuals should formally submit requests for network and system access and obtain explicit approval.
Ongoing Monitoring and Review of Access	Individuals' access needs are expected to change over time. Access should be reviewed at least annually, or immediately if an individual's need to know changes (e.g., if they change job functions).
Access Removal	Individuals who no longer work for an organization should have their access privileges removed immediately. Access privileges should also be immediately terminated if an employee's job functions have changed such that they no longer require access to the level at which privileges were previously granted.
Least Privilege Access	Each user in a system should be granted the most restrictive set of privileges (or lowest access) needed to perform authorized tasks. This limits the damage that can result from an accident, error, or unauthorized use.

Source: DHS criteria[6]

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

[6] DHS *4300A Sensitive Systems Handbook,* Version 12.0, November 15, 2015, provided the requirements we used for our audit. On September 20, 2022, DHS rescinded the handbook and replaced it with a new policy directive, DHS 4300A, *Information Technology Systems Security Program, Sensitive Systems*, Version 13.2.

In addition to using access controls, organizations can improve their ability to withstand cyberattacks by promptly addressing vulnerabilities and using appropriate security settings. Such practices increase security awareness and minimize risks to systems by identifying, managing, and tracking security risks and threats until they are addressed.

ICE is responsible for investigating transnational crime and threats, specifically those from criminal organizations that seek to exploit the global infrastructure through which international trade, travel, and finance move. ICE has more than 20,000 law enforcement and support personnel in more than 400 offices in the United States and around the world. Given the vast amount of data that ICE maintains, as well as ICE's important law enforcement mission, it is vital that the component have effective access controls to accomplish its mission securely and efficiently.

ICE's Administration of Information Technology (IT) Access Controls

ICE's Office of the Chief Information Officer (OCIO) provides IT services and capabilities to support ICE's mission. Accordingly, OCIO has developed a number of critical IT initiatives to help ICE modernize its IT systems, update its IT management disciplines, and provide IT solutions throughout the component. ICE has an official account and access management system for creating, maintaining, and disabling Active Directory accounts. This system helps to ensure access requests are reviewed and formally approved by the appropriate individuals.

ICE's general support systems[7] for providing capabilities to accomplish mission critical tasks and meet IT infrastructure requirements include the following:

- ICE Enterprise Network is ICE's IT infrastructure, including servers, routers, switches, and firewalls.

- ICE Workstations System consists of approximately 34,600 workstations (laptops, desktops) inside the ICE Enterprise Domain environment.

As shown in in Table 2, ICE has established two primary types of IT user accounts for managing access controls: (1) general user and (2) privileged user.

[7] General support systems are an interconnected set of information resources under the same direct management control that share common functionality. They normally include hardware, software, information, data, and applications.

Table 2. Overview of ICE User Account Types

ICE Account Type	Description
General User Account	Used for routine job functions such as email, web browsing, and using line of business applications.
Privileged User Account	Authorized to perform security functions that ordinary users cannot perform, such as network system administration and system maintenance.

Source: ICE criteria

We conducted this audit to determine the extent to which ICE applied IT access controls to restrict unnecessary access to systems and information. This audit is one of three in a series of audits for access controls of DHS components; two audits were conducted in 2022 on U.S. Citizenship and Immigration Services (USCIS)[8] and Federal Emergency Management Agency (FEMA)[9] access controls.

Results of Audit

ICE did not consistently implement effective access controls to restrict access to its network and IT systems. Although ICE took a multi-layered approach to managing access for personnel who change positions or leave the component altogether, we determined that ICE did not consistently manage or remove access when personnel separated or changed positions. For example, 84 percent of the accounts for separated personnel we examined remained active beyond the individual's last workday. Additionally, ICE did not monitor and configure privileged user access, service accounts, and access to sensitive security functions as required. These deficiencies stemmed from insufficient internal controls and oversight of user account management and compliance to ensure access controls were administered appropriately and effectively to prevent unauthorized access.

[8] *USCIS Should Improve Controls to Restrict Unauthorized Access to Its Systems and Information*, OIG-22-65, September 7, 2022.
[9] *FEMA Should Improve Controls to Restrict Unauthorized Access to Its Systems and Information*, OIG-23-16, February 15, 2023.

Based on our testing, ICE did not implement all security settings for its IT systems and workstations because it was concerned that these settings negatively impacted system operations. In addition, according to officials, ICE accepted the risk of not implementing the required settings but did not provide any supporting evidence.

The deficiencies identified during this audit exposed ICE's network and IT systems to risks of compromise by potential attackers. ICE is taking steps to enhance its access control processes. However, until these deficiencies are addressed, ICE's network and IT systems remain at risk. Additionally, these deficiencies could have limited the Department's overall ability to reduce the risk of unauthorized access to its network, which may disrupt mission operations.

ICE Did Not Effectively Manage Access to Its Network and IT Systems

ICE has a multi-layered approach to managing network and IT system access, but it did not consistently manage or remove access when personnel separated or changed positions. Additionally, ICE did not meet requirements for monitoring and assigning privileged user access and for monitoring and configuring service accounts. We attribute these deficiencies to insufficient internal controls and oversight of user account management and compliance to ensure access controls were administered appropriately and effectively to prevent unauthorized access.

ICE Did Not Appropriately Remove or Verify Access for Separated and Transferred Personnel

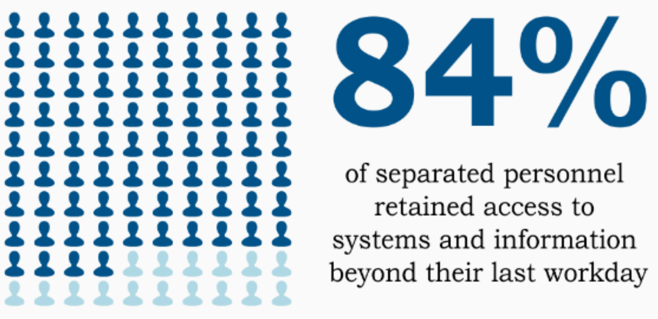
Removing access for separated and transferred personnel is an effective method for preventing individuals who no longer have a mission need from accessing system resources. At the time of our audit, *DHS 4300A Sensitive Systems Handbook*[10] required system administrators to immediately terminate IT access of separated and transferred personnel who no longer need access to perform their duties. Additionally, ICE is required to adhere to its *ICE System Security Plan for Active Directory Exchange*, April 25, 2022, as guidance for disabling user accounts. However, ICE did not consistently manage or remove access for personnel who separated and transferred.

[10] *DHS 4300A Sensitive Systems Handbook,* Version 12.0, November 15, 2015.

Management of Account Access for Separated Individuals

Although system administrators are responsible for immediately disabling general access for separated personnel, 84 percent of the accounts in our sample[11] of separated personnel remained active beyond the individual's last workday. In other words, 159 of 190 separated personnel in our sample population had access to ICE's systems and information beyond their last workday, as shown in Figure 1. Of the 159 accounts that were not promptly deactivated, 25 (16 percent) maintained access to ICE's network for 45 days or longer.

Figure 1. Separated Personnel Who Retained General System Access



Source: DHS Office of Inspector General, based on judgmental sample of ICE data

These 159 accounts for separated personnel remained active because ICE supervisors and system administrators did not correctly follow procedures for disabling the access as required. According to ICE procedures,[12] when individuals separate from ICE, their supervisors must submit requests for their accounts to be immediately disabled. Supervisors or system administrators did not submit these requests for 159 of 190 accounts (84 percent) we tested. In these cases, ICE relied on system controls to disable the accounts: ICE's system runs a script to detect and automatically disable the accounts of users who have not logged into an ICE system in more than 45 days. Although ICE used these backup controls to deactivate accounts, 25 accounts in our sample had not been disabled by the system script after 45 days.

Additionally, ICE did not monitor user accounts as required by DHS security policy. Although ICE system owners and supervisors performed reviews for some systems, we found that these reviews were not consistent. For example, ICE's *Office of the Principal Legal Advisor Case Management System PLAnet*

[11] We tested a judgmental sample of the 190 individuals who separated from ICE from January 14, 2022, through June 27, 2022. ICE was only able to provide data for approximately a 180-day period for separated personnel as ICE does not maintain archival data on separated employees for longer than 6 months.
[12] *ICE OCIO IRMnet Account Management Procedure,* October 15, 2019.

Access Controls Procedures[13] require quarterly reviews of all active accounts and users' roles to verify the validity of user accounts and accuracy of assigned permissions. While ICE officials conducted reviews more frequently than the required quarterly reviews, we found 65 of 1,931 (3 percent) users[14] still had access after their Active Directory accounts had been disabled. An ICE official stated that this occurred due to human error.

We reported similar findings in two prior audits of USCIS[15] and FEMA[16] access controls. USCIS and FEMA did not consistently apply the IT access controls needed to restrict unnecessary access to their systems, networks, and information. We reported that both components were also overly reliant on backup mechanisms to disable accounts and did not follow their own procedures.

We also reported similar findings in a prior audit[17] of the Department's use of personal identity verification cards and security clearances to control access to its systems and facilities. Specifically, DHS did not always terminate personal identity verification card access or withdraw security clearances for separated employees and contractors in accordance with Federal regulations and departmental policies.

Management of Account Access for Transferred Individuals

We identified 6,134 individuals who transferred offices within ICE from May 2021 through May 2022. From a random sample of 204, we judgmentally sampled 39 special agents who changed from supervisory to non-supervisory positions.[18] We submitted the sample to ICE to review the agents' access to its Investigative Case Management system.[19] ICE could not demonstrate that it had removed supervisory permissions for the sampled individuals. Therefore,

[13] ICE's *Office of the Principal Legal Advisor Case Management System PLAnet Access Controls Procedures*, Version 2, December 3, 2021. PLAnet stands for Principal Legal Advisor Network.
[14] ICE provided the audit team a list that contained all Office of the Principal Legal Advisor Case Management System PLAnet users.
[15] *USCIS Should Improve Controls to Restrict Unauthorized Access to Its Systems and Information,* OIG-22-65, September 7, 2022.
[16] *FEMA Should Improve Controls to Restrict Unauthorized Access to Its Systems and Information,* OIG-23-16, February 15, 2023.
[17] *DHS Did Not Always Promptly Revoke PIV Card Access and Withdraw Security Clearances for Separated Individuals,* OIG-23-04, December 20, 2022.
[18] ICE special agents had instances of temporary promotions or special assignments that required supervisory access to ICE systems. Once the temporary promotion or special assignment was over, the agents retained supervisory access.
[19] ICE's Investigative Case Management application is the primary law enforcement case management system used by ICE Homeland Security Investigations special agents and personnel to manage civil law enforcement activities and to support criminal prosecutions.

we determined that all 39 special agents still had supervisory permissions within ICE's Investigative Case Management system.

This occurred because ICE did not have a policy or process to identify and enforce access changes that may be needed when an individual transfers within the component. ICE had a policy for disabling the accounts of separating employees,[20] but not a policy or process to ensure unneeded access was removed when individuals transferred offices. Instead, each transferred employee's supervisor and each IT system administrator[21] were expected to proactively identify transferred personnel whose access should be reviewed.

ICE Did Not Adequately Assign and Monitor Privileged User Access

ICE's privileged users are trusted to perform critical IT security functions and may be granted powerful (i.e., high-level) access to sensitive assets. Attackers covet privileged accounts because of the broad access typically granted to these accounts. Accordingly, DHS IT security policy[22] requires that privileged access be restricted only to users who have a mission need. Because access needs may change over time, ICE's system security plans[23] require that system owners and supervisors review all privileged accounts annually to ensure higher levels of access continue to be appropriate.

ICE did not limit privileged access to only those accounts that had a mission need. Specifically, ICE inappropriately granted 116 of 47,810 general user accounts the ability to access sensitive security accounts and allow for domain compromise by escalating privileges directly through active directory permissions, such as resetting account passwords and/or allowing for domain replication permissions. These sensitive security accounts are used to manage access across the component, but these users had no mission need for this access. ICE officials explained that the 116 accounts received this access by mistake — they had inherited the permission to reset the password to the

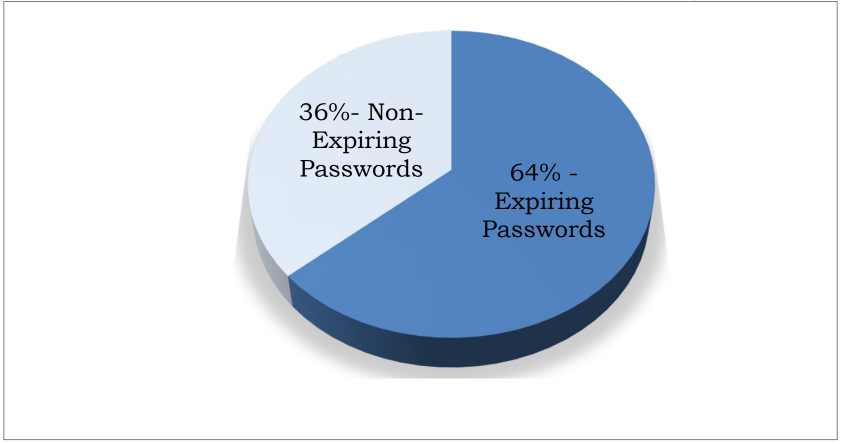
[20] *ICE System Security Plan for Active Directory Exchange*, April 25, 2022.
[21] System Administrators are personnel who manage access controls.
[22] *DHS Sensitive Systems Policy Directive 4300A*, Version 13.1, July 27, 2017, provided the requirements we used for our audit. DHS published a new policy directive, DHS 4300A, *Information Technology Systems Security Program, Sensitive Systems*, Version 13.2, on September 20, 2022.
[23] We reviewed multiple system security plans for systems that had privileged user accounts.

security account indirectly through another permission that was previously approved for the accounts.

ICE Did Not Adequately Manage and Monitor Service Account Access

ICE uses 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 automated[24] and may have highly privileged access. ICE did not monitor service accounts as required. For example, DHS Change Memorandum 13.1.1 to *DHS Sensitive Systems Policy Directive 4300A*[25] required that service account passwords be changed annually to reduce the risk of unauthorized access. However, 549 of 1,509[26] (36 percent) ICE enabled service accounts were configured to have non-expiring passwords (see Figure 2). ICE did not have a process to review service account passwords as required because it had an internal policy[27] to use non-expiring passwords for service accounts. During our audit, ICE stated that it has created an ICE Service Account Working Group to determine a solution for managing service accounts and passwords.

Figure 2: ICE Service Accounts with Non-Expiring Passwords



Source: DHS OIG, based on Active Directory scans and ICE documentation

[24] Service accounts run automated business processes and are used by applications, not people.
[25] Change Memorandum 13.1.1 to *DHS Sensitive Systems Policy Directive 4300A*, October 2, 2019, provided the requirements used for our audit. DHS published a new policy directive, DHS 4300A *Information Technology Systems Security Program, Sensitive Systems*, Version 13.2. on September 20, 2022.
[26] ICE had a total of 1,509 enabled service account within the IRMnet domain that were scanned for expiring passwords.
[27] *ICE Active Directory Exchange Service Account Creation.*

DHS components with systems requiring encryption must comply with Federal guidelines.[28] We identified inadequately managed service accounts that were susceptible to password compromise. Specifically, these 816 accounts were associated with a Service Principal Name[29] and used weak encryption, which made them vulnerable to a password compromise type of attack known as "Kerberoasting."[30] Although ICE has implemented a control to force all newly created accounts to require strong Advanced Encryption Standard 256-bit encryption, it could not do so for legacy accounts. ICE officials stated that previous attempts to strengthen encryption for legacy accounts had negatively affected applications and operations. Officials in ICE's OCIO stated that they are aware of this issue and are reviewing ICE accounts that are associated with Service Principal Names to correct the weak encryption configuration.

ICE Did Not Implement Required Settings and Address IT Infrastructure and Workstation Vulnerabilities

DHS relies on configuration and vulnerability management programs to identify, manage, and resolve threats to its systems and network. Fully updated and hardened systems adhering to DHS requirements ensure stronger access controls and significantly reduce DHS' risk of compromise. Although ICE's systems and workstations generally complied with DHS' security standards,[31] ICE did not implement all required settings and address vulnerabilities in a timely manner in accordance with the DHS Enterprise Security Operations Center's Information Security Vulnerability Management notices.[32] After initially testing configuration settings, ICE officials expressed concerns that these settings impacted system operations. In addition, according to officials, ICE accepted the risk of not implementing the required settings.

[28] *DHS Sensitive Systems Policy Directive 4300A,* Version 13.1, July 27, 2017, required that all accounts use Advanced Encryption Standard 256-bit encryption.

[29] A Service Principal Name is the unique identifier for a Windows service instance. These services are associated with a service account that has permission to identify and authenticate or start that service.

[30] Kerberoasting is a password compromise attack that attempts to crack the password of a service account. Once an attacker has the password, they can obtain elevated privileges to control servers and move through networks, creating backdoors for future attacks and stealing data.

[31] *DHS Sensitive Systems Policy Directive 4300A,* Version 13.1, July 27, 2017, required components to manage systems to reduce vulnerabilities through vulnerability testing and management, promptly installing patches and eliminating or disabling unnecessary services.

[32] Information Security Vulnerability Management notices provide notification of newly discovered vulnerabilities and tracks the status of vulnerability resolution.

ICE Did Not Promptly Update Its IT Infrastructure and Workstations to Address Known Vulnerabilities

DHS components must address vulnerabilities in their systems by installing appropriate patches according to timeframes published through the DHS Enterprise Security Operations Center's Information Security Vulnerability Management notices. We determined that ICE did not remediate all critical and high-risk vulnerabilities in its IT enterprise within DHS' required timelines. We conducted vulnerability scans of six unique ICE IT assets and identified critical and high-risk vulnerabilities on domain controllers, servers, and workstations. Our scans of one ICE system identified five unique critical vulnerabilities (with 28 occurrences) and 27 unique high-risk vulnerabilities (with 620 occurrences) for which remediation was overdue. For example, one critical vulnerability should have been remediated by November 15, 2018, but was outstanding at the time of our scan on July 19, 2022. For the other systems scanned, ICE was missing three unique critical updates (with 8 occurrences) and four unique high-risk updates (with 15 occurrences).

According to ICE OCIO, because ICE systems are geographically dispersed throughout the world, software updates take time to reach all endpoints. ICE officials stated that they are correcting vulnerabilities as required by the *DHS Plan of Action and Milestone Guide*[33] to track, manage, and mitigate the risk of identified weaknesses of DHS systems.

ICE Did Not Implement All Required Security Settings

According to DHS 4300A, components must use system security settings that are consistent with the Defense Information Security Agency's (DISA) *Security Technical Implementation Guides* (STIGs).[34] Under this policy, DHS components have 135 calendar days to ensure their system security settings comply with the DISA STIG. If a system is not in compliance, the component must create and submit a system-level Plan of Action and Milestones to DHS. If a component cannot implement all required settings, then it can request an exception via a waiver. We requested waivers and risk acceptance documentation as compensating managerial controls, but ICE did not provide any supporting evidence.

[33] The *DHS Plan of Action and Milestone Guide* (Attachment H of DHS 4300A, *Information Technology System Security Program, Sensitive Systems*) outlines the requirements for developing, maintaining, closing, and reporting program and system level weaknesses and deficiencies to DHS for all information systems and programs supporting DHS.
[34] DISA STIG are configuration standards for devices and systems developed by the DISA to safeguard the U.S. Department of Defense IT network and systems.

Our scans of two ICE systems revealed that ICE did not fully implement all DISA STIG security settings. Although ICE's compliance with the DISA STIG varied for the two systems we scanned (see Table 3), four of the six IT assets in these two systems contained settings that fall into the highest category of vulnerabilities.

Table 3. ICE DISA STIG Compliance

IT Asset	Number of Assets Tested	Compliance	Number of Settings Tested	Number of Failed Settings	CAT 1 Unique Failed Settings[35]
IT Asset 1	383	83%	102,839	17,966	10
IT Asset 2	1	40%	290	175	0
IT Asset 3	9	81%	1,922	365	3
IT Asset 4	7	84%	1,699	271	3
IT Asset 5	106	73%	26,402	7,143	1
IT Asset 6	2	67%	544	179	1

Source: DHS OIG, based on ICE system scans

ICE was aware of its noncompliance and explained that it was concerned that implementing all required DISA STIG settings might disrupt system operations, resulting in ICE being unable to support its end users. After obtaining our results, ICE created a Plan of Action and Milestones to address the noncompliance by July 28, 2023. The plan will have system teams configure all applicable assets with the remaining DISA STIG settings to meet DHS 4300A configuration hardening requirements.

Conclusion

ICE's access control deficiencies increase the risk that unauthorized individuals could gain access to sensitive information, including the personally identifiable information and criminal data that ICE collects to support immigration and law enforcement organizations. ICE's inadequate security settings on systems and workstations may limit its ability to overcome a major cybersecurity incident or to mitigate an access control weakness if an unauthorized individual gains access. DHS' overall security posture relies on all components to implement effective IT security processes. Therefore, ICE's

[35] DISA Category 1 vulnerability refers to any vulnerability that will directly and immediately result in loss of confidentiality, availability, or integrity. These vulnerabilities can allow unauthorized access to classified data or facilities and can lead to a denial of service or access.

access control and system security deficiencies may limit the Department's ability to reduce the risk of unauthorized access to its network and disruption of mission operations.

Recommendations

Recommendation 1: 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.

Recommendation 2: 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.

Recommendation 3: 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.

Recommendation 4: 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.

Recommendation 5: 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.

Recommendation 6: We recommend the ICE Office of the Chief Information Officer develop and implement measures to ensure service account passwords are updated as required.

Recommendation 7: 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.

ICE Comments and OIG Analysis

We obtained written comments on a draft of this report from ICE.

We reviewed ICE's management comments, as well as the technical comments previously submitted and updated the report as appropriate. Recommendations 1 through 7 are resolved and open. In the comments, ICE indicated it appreciated our work on this audit. ICE stated that it remains committed to continuous improvement and implementation of access control and account management strategies across the component. A summary of ICE responses and our analysis follows.

ICE Response to Recommendation 1: Concur. ICE will enforce compliance through communication and training to stakeholders to ensure all separated employees are removed from enterprise and system account management groups and access control lists. ICE is actively implementing an Account Lifecycle Management (ALM) solution to further automate account management capabilities. As part of the overall ALM solution, ICE OCIO will implement a process to notify stakeholders when an employee separates from ICE and trigger the appropriate action. In addition, OCIO will develop and implement an Enterprise Account Management standard, to include guidance on implementing the existing DHS policy, by October 30, 2023. OCIO will also refine the Security Role Based Training, Information System Security Office Training, and Cyber Security Annual Training to include guidance on removing separated employees' access to all ICE systems, networks, and applications in accordance with DHS policy by December 31, 2023. Estimated Completion Date (ECD): June 28, 2024.

OIG Analysis: ICE's actions are responsive to this recommendation, which will remain open and resolved until ICE provides documentation showing it has developed and implemented its ALM solution; updated guidance on DHS policy implementation; and updated training to include guidance on removing separated employees' access to all ICE systems, networks, and applications.

ICE Response to Recommendation 2: Concur. ICE will enforce compliance through communication and training to stakeholders to ensure all transferred employees are updated in enterprise and system account management groups and access control lists. Specifically, ICE will implement an ALM solution to further automate account management capabilities. As part of the overall ALM solution, ICE will implement a process to identify employees transferring roles within the component. In addition, ICE OCIO will develop and implement an Enterprise Account Management standard, to include guidance on implementing existing DHS policies, by October 30, 2023. OCIO will also refine the Security Role Based Training, Information System Security Office Training, and Cyber Security Annual Training to include guidance on identifying all transferred employees and ensuring their user group access is reviewed and verified immediately at the end of their prior position in accordance with DHS policy, by December 31, 2023. ECD: June 28, 2024.

OIG Analysis: ICE's actions are responsive to this recommendation, which will remain open and resolved until ICE provides documentation showing it has developed and implemented its ALM solution; implemented its Enterprise Account Management standard; and updated guidance on reviewing and verifying transferred employees' access to all ICE systems, networks, and applications.

ICE Response to Recommendation 3: Concur. ICE OCIO will develop and implement an Enterprise Account Management standard, to include guidance on implementing existing DHS policies. This will include a review of current access management procedures to ensure privileged and general user accounts meet DHS policy and are reviewed per documented timelines. ICE will further enforce compliance of privileged users through stakeholder communication and training to ensure all employees are updated in enterprise and system account management groups and access control lists. For service accounts, ICE will deploy an automated service account credential management solution, which will reduce reliance on human intervention, to manage service account credentials. All ICE Enterprise Infrastructure Defense Group managed service accounts have been migrated to group managed service accounts (GMSA) or are being vaulted by the CA Privileged Access Manager (PAM). Active Directory enterprise accounts are also being migrated to GMSAs or being vaulted by August 31, 2023. In addition, the OCIO Active Directory team is documenting a procedure for onboarding member server applications into the GMSA or CA PAM service account vaulting solutions by September 30, 2023. Once the new procedure is approved, ICE will begin onboarding application service accounts. ECD: June 28, 2024.

OIG Analysis: ICE's actions are responsive to this recommendation, which will remain open and resolved until ICE provides documentation showing it has implemented its Enterprise Account Management standard, updated guidance and training on enterprise and system account management groups and access control lists for employees, and deployed an automated service account credential management solution.

ICE Response to Recommendation 4: Concur. ICE Domain and Security administrative rights have been fully restructured to comply with DHS policy on having accounts with the fewest privileges necessary. In addition, the IRMnet Account Management Procedure document is being updated to reflect the restructuring of administrative rights, and procedural artifacts will be updated, as appropriate. Once this is complete, ICE will review account permissions and will update or remove account permissions as necessary. ECD: January 31, 2024.

OIG Analysis: ICE's actions are responsive to this recommendation, which will remain open and resolved until ICE provides documentation showing it has updated the IRMnet Account Management Procedure document and reviewed and updated or removed account permissions after the document is updated.

ICE Response to Recommendation 5: Concur. ICE OCIO will review service accounts to identify accounts that do not align with DHS policy requirements, and corrective action will be taken to bring accounts into compliance. If corrective actions cannot be taken, waivers or risk acceptance memoranda will be submitted for noncompliant configurations. ECD: November 30, 2023.

OIG Analysis: ICE's actions are responsive to this recommendation, which will remain open and resolved until ICE provides documentation showing it has taken corrective action to bring accounts into compliance or provided waivers/risk acceptance memoranda if corrective action cannot be taken.

ICE Response to Recommendation 6: Concur. ICE OCIO will develop and implement an Enterprise Account Management standard, to include guidance on implementing existing DHS policies. ICE will also deploy an automated service account credential management solution, reducing reliance on human intervention, to manage service account credentials. Further, all ICE Enterprise Infrastructure Defense Group managed service accounts have migrated to GMSAs or are being vaulted by the CA PAM. Active Directory enterprise accounts are being migrated to GMSAs or vaulted by August 31, 2023. In addition, the OCIO Active Directory team is documenting a procedure for onboarding member server applications into the GMSA or CA PAM service account vaulting solutions by September 30, 2023. Once the new procedure is approved, ICE will begin onboarding application service accounts. ECD: June 28, 2024.

OIG Analysis: ICE's actions are responsive to this recommendation, which will remain open and resolved until ICE provides documentation showing it has implemented its Enterprise Account Management standard, deployed an automated service account credential management solution, migrated accounts, and updated procedures.

ICE Response to Recommendation 7: Concur. ICE OCIO will implement several approaches to improve Windows vulnerability management across the enterprise. These approaches will focus on Windows workstation patching improvements, Windows workstation configuration setting improvements, and

Windows server configuration improvements. In addition, OCIO will develop and implement an enterprise vulnerability management standard, to include guidance on implementing existing DHS policies by November 30, 2023. Concurrently, OCIO will maximize coverage of existing vulnerability remediation solutions to enhance reporting and automated remediation of devices found to be out of compliance. ECD: March 29, 2024.

OIG Analysis: ICE's actions are responsive to this recommendation, which will remain open and resolved until ICE provides documentation showing it has implemented approaches to improve Windows vulnerability management across the enterprise, as well as developed and implemented an enterprise vulnerability management standard.

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*.

We conducted this audit to determine the extent to which ICE is applying IT access controls to restrict unnecessary access to systems and information. We evaluated ICE's account management processes for authorizing, validating, and disabling users' access. We also performed technical assessments of ICE's domain and selected systems to identify weaknesses and security risks. Additionally, we assessed internal controls and compliance with applicable policies and procedures necessary to satisfy the audit. In particular, we assessed information system control effectiveness. However, because our review was limited to these internal control components and underlying principles, it may not have disclosed all internal control deficiencies that may have existed at the time of this audit.

To conduct this audit, we gathered system documentation related to access control implementation and evidence of access control–related actions for creating, disabling, and validating user accounts. In addition, we reviewed and analyzed relevant system security plans. We researched and used Federal and departmental criteria for access control requirements. We observed IT systems to understand ICE's processes for creating, disabling, and validating accounts. We interviewed system owners; information system security officers; and personnel from ICE's Workforce Management Branch, Office of the Chief Information Security Officer, and Resource Management Division. We relied on the work of internal specialists from DHS OIG's Office of Innovation, Cybersecurity Risk Assessment Division, to perform technical assessments of ICE's systems and domain. Specifically, they assessed selected systems and a statistically valid sample of workstations to determine how ICE manages vulnerabilities and security settings. The internal specialists also completed an Active Directory assessment scan of ICE's network. We used the information obtained from these assessments to identify system vulnerabilities such as missing security updates, misconfigured security settings, the presence of unsupported operating systems, and Active Directory weaknesses or misconfigurations.

We also obtained data from ICE OCIO's Enterprise Services Branch and Office of Human Capital to identify personnel who separated from ICE or transferred within the component from January 14, 2022, through June 27, 2022, and May 2021 through April 2022, respectively. After assessing the reliability of the data, we determined the data was sufficiently reliable for our audit purposes. From this data, we identified a population of 1,389 separated individuals and selected a judgmental sample of 190 for our testing. Additionally, we identified a population of 6,134 individuals who experienced internal personnel actions within ICE during the same timeframe and selected a judgmental sample of 39 for our testing.

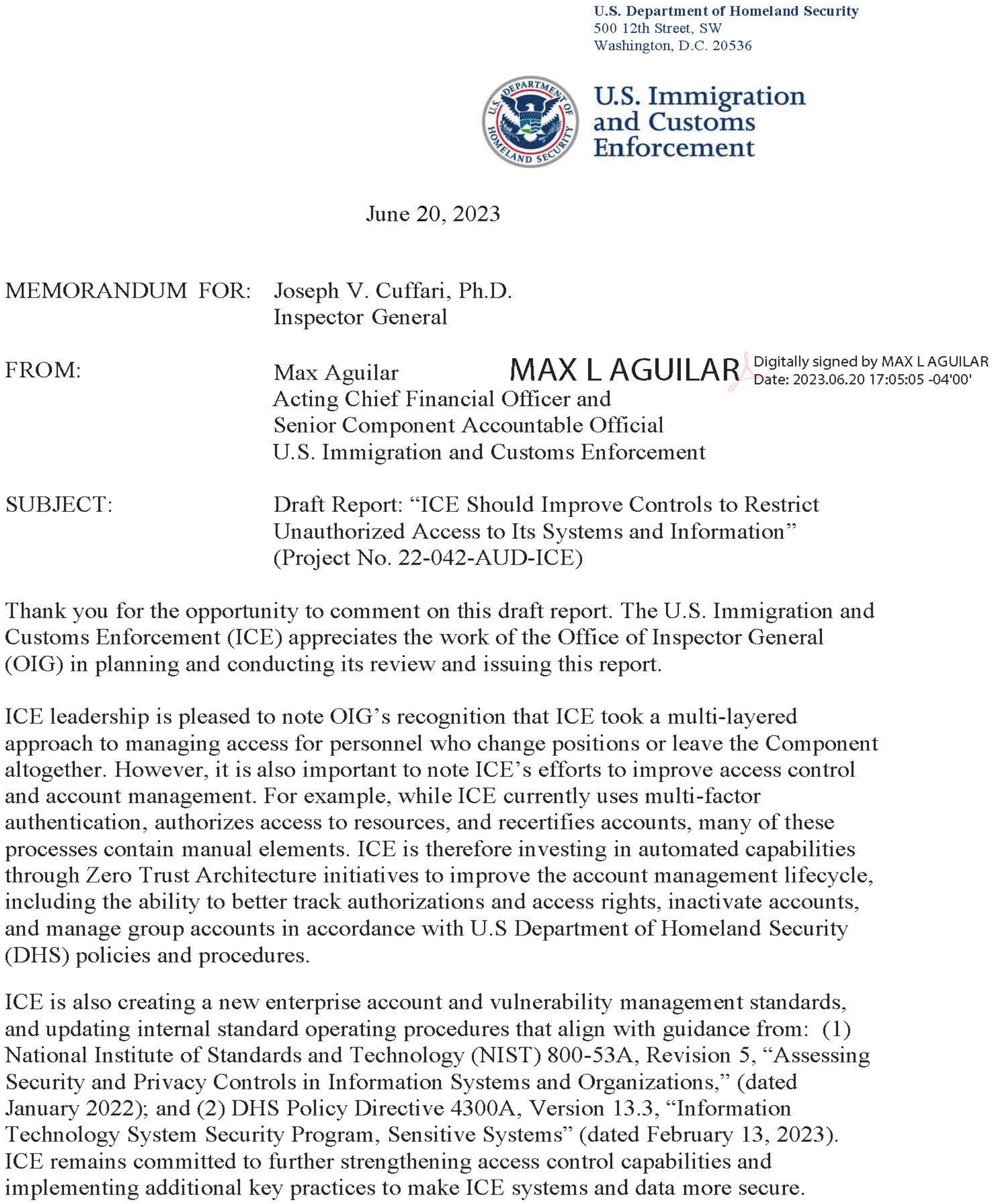
To ensure the accuracy of our testing results and reporting, we gave ICE the opportunity to review our preliminary observations, verify the initial results, and identify “false-positive” results. We reviewed ICE’s feedback and updated our analysis as needed.

We conducted this performance audit between April 2022 and February 2023 pursuant to the *Inspector General Act of 1978*, *as amended*, and according to generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

DHS OIG Access to DHS Information

During this audit, DHS provided timely responses to DHS OIG’s requests for information and did not delay or deny access to information we requested.

Appendix B
ICE Comments to the Draft Report



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

U.S. Immigration
and Customs
Enforcement

June 20, 2023

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

FROM: Max Aguilar MAX L AGUILAR Digitally signed by MAX L AGUILAR Date: 2023.06.20 17:05:05 -04'00'
Acting Chief Financial Officer and
Senior Component Accountable Official
U.S. Immigration and Customs Enforcement

SUBJECT: Draft Report: "ICE Should Improve Controls to Restrict Unauthorized Access to Its Systems and Information" (Project No. 22-042-AUD-ICE)

Thank you for the opportunity to comment on this draft report. The 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 took a multi-layered approach to managing access for personnel who change positions or leave the Component altogether. However, it is also important to note ICE's efforts to improve access control and account management. For example, while ICE currently uses multi-factor authentication, authorizes access to resources, and recertifies accounts, many of these processes contain manual elements. ICE is therefore investing in automated capabilities through Zero Trust Architecture initiatives to improve the account management lifecycle, including the ability to better track authorizations and access rights, inactivate accounts, and manage group accounts in accordance with U.S Department of Homeland Security (DHS) policies and procedures.

ICE is also creating a new enterprise account and vulnerability management standards, and updating internal standard operating procedures that align with guidance from: (1) National Institute of Standards and Technology (NIST) 800-53A, Revision 5, "Assessing Security and Privacy Controls in Information Systems and Organizations," (dated January 2022); and (2) DHS Policy Directive 4300A, Version 13.3, "Information Technology System Security Program, Sensitive Systems" (dated February 13, 2023). ICE remains committed to further strengthening access control capabilities and implementing additional key practices to make ICE systems and data more secure.

The draft report contained seven recommendations with which ICE concurs. Enclosed find our response to each recommendation. ICE previously submitted technical comments addressing several accuracy, contextual, and other issues under a separate cover for OIG's consideration.

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

Enclosure

Enclosure: Management Response to Recommendations Contained in 22-042-AUD-ICE

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

Recommendation 1: Develop and implement processes to remove separated employees' access to all ICE systems, networks, and applications in accordance with DHS policy.

Response: Concur. ICE will enforce compliance through communication and training to stakeholders to ensure all separated employees are removed from enterprise and system account management groups and access control lists. ICE is actively implementing an Account Lifecycle Management (ALM) solution, via SailPoint software, to further automate account management capabilities – Creation, Review/Update, and Deactivation (CRUD). As part of the overall ALM capability, ICE OCIO will implement a process to notify stakeholders when an employee separates from ICE and trigger the appropriate action. In addition, the OCIO will develop and implement an Enterprise Account Management standard, to include guidance on the implementation of the existing DHS policy by October 30, 2023. OCIO will also refine the Security Role Based Training, Information System Security Officer (ISSO) Training, and Cyber Security Annual Training (CSAT) to include guidance on removing separated employees' access to all ICE systems, networks, and applications in accordance with DHS policy by December 31, 2023. Estimated Completion Date (ECD): June 28, 2024.

Recommendation 2: 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.

Response: Concur. ICE will enforce compliance through communication and training that stakeholders ensure all transferred employees are updated in enterprise and system account management groups and access control lists. Specifically, ICE will implement an ALM solution via SailPoint software to further automate account management capabilities – CRUD. As part of the overall ALM capability, ICE will implement a process to identify employees transferring roles within ICE. In addition, the ICE OCIO will develop and implement an Enterprise Account Management standard, to include guidance on the implementation of the existing DHS policies, by October 30, 2023. In the interim, OCIO is also refining the Security Role Based Training, ISSO Training, and CSAT to include guidance 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, by December 31, 2023. ECD: June 28, 2024.

Recommendation 3: Develop and implement a repeatable process to conduct and monitor privileged user and service account reviews in accordance with DHS policy.

Response: Concur. ICE OCIO will develop and implement an Enterprise Account Management standard, to include guidance on the implementation of existing DHS policies. This will include a review of current access management procedures to ensure privileged and user accounts meet DHS policy and are reviewed per documented timelines. ICE will further enforce compliance of privileged users through stakeholder communication and training to ensure all employees are updated in enterprise and system account management groups and access control lists.

For service accounts, ICE will deploy an automated service account credential management solution, which will reduce reliance on human intervention, to manage service account credentials. All ICE Enterprise Infrastructure Defense Group (IDG) managed service accounts have migrated to group managed service accounts (GMSA) or are being vaulted by CA Privileged Access Manager (PAM). Active Directory enterprise accounts are also in the process of migrating to GMSA or being vaulted by August 31, 2023. In addition, the OCIO Active Directory team is documenting a procedure for onboarding member server applications into the GMSA or CA PAM service account vaulting solutions by September 30, 2023. Upon approval of the new procedure, ICE will begin onboarding application service accounts. ECD: June 28, 2024.

Recommendation 4: Remove the unnecessary privileges that allow additional users to access the sensitive security accounts we identified.

Response: Concur. ICE Domain and Security Admin rights have been fully restructured to comply with the least privilege accounts in accordance with DHS policy. In addition, the IRMnet Account Management Procedure document is being updated to reflect the restructuring of administrative rights, and procedural artifacts will be updated, as appropriate. Once this is complete, ICE will review account permissions and will update/remove account permission, as necessary. ECD: January 31, 2024.

Recommendation 5: 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.

Response: Concur. ICE OCIO will review service accounts to identify accounts that do not align with DHS policy requirements, and corrective action will be taken to bring accounts into compliance. If corrective actions cannot be taken, waivers/risk acceptance memos will be submitted for non-compliant configurations. ECD: November 30, 2023.

Recommendation 6: Develop and implement measures to ensure service account passwords are updated as required.

Response: Concur. ICE OCIO will develop and implement an Enterprise Account Management standard, to include guidance on the implementation of the existing DHS policies. ICE will also deploy an automated service account credential management solution, reducing reliance on human intervention, to manage service account credentials. Further, all ICE Enterprise IDG managed service accounts have migrated to GMSA or are being vaulted by CA PAM. Active Directory enterprise accounts are in process of migrating to GMSA or vaulted by August 31, 2023. In addition, the OCIO Active Directory team is documenting a procedure for onboarding member server applications into the GMSA or CA PAM service account vaulting solutions by September 30, 2023. Upon approval of the new procedure, ICE will begin onboarding application service accounts. ECD: June 28, 2024.

Recommendation 7: Evaluate its vulnerability management program to identify and implement automated tools to help address known vulnerabilities within required timeframes.

Response: Concur. The ICE OCIO will implement several approaches to improve Windows Vulnerability Management across the enterprise:

1. Windows workstation patching improvements, to include:
   a. Continuing to replace end of life workstations, which will reduce security vulnerabilities and improve application of Operating System patches;
   b. Migrating to Adaptiva Cloud, to allow off network patching;
   c. Configuring shortened timelines for installation of patches, which will reduce device reboot times from 10 hours to 7 hours;
   d. Implementing changes to Microsoft deployments by separating out Microsoft application patching from operating system security patching; and
   e. Investing in technology such as Axonious to provide timely patch reporting and compliance numbers.

2. Windows workstation configuration setting improvements, to include:
   a. Reviewing enterprise encryption standards and deconflicted Group Policy Settings (GPOs) to improve "category 1, 2 and 3" compliance with the Defense Information Security Agency's (DISA) Security Technology Implementation Guide (STIG) for Windows 10 devices;
   b. Developing a Windows 11 migration plan that includes an update Workstation DISA STIG GPOs, as the Windows 11 migration is scheduled

Management Response to Draft Report: "ICE Should Improve Controls to Restrict Unauthorized Access to Its Systems and Information" (Project No. 22-042-AUD-ICE)
Page 6

to start no later than January 30, 2024, pending inoperability testing on all ICE applications.

3. Windows server configurations improvements, to include:
   a. Implementing a new GPO to increase Windows server 2022 STIG compliance; and
   b. Continuing to deconflict GPOs and Active Directory Organizational Units to resolve lingering compliance issues with member servers.

In addition, the OCIO will develop and implement an enterprise vulnerability management standard, to include guidance on the implementation of existing DHS policies by November 30, 2023. Concurrently, OCIO will also maximize coverage of existing vulnerability remediation solutions to enhance reporting and automated remediation of devices found to be out of compliance. ECD: March 29, 2024.

Appendix C
Office of Audits Major Contributors to This Report

Tarsha Cary, Director
Danny Urquijo, Audit Manager
Robert Williams, Auditor-in-Charge
Brandon Hoel, Auditor
Zachary Israel, Auditor
Saad Amjed, IT Specialist
Usman Mohammed, IT Specialist
Maria Romstedt, Communications Analyst
Helen White, Independent Referencer

Office of Innovation, IT and Data Specialist Support

Cybersecurity Risk Assessment
Thomas Rohrback, Director
Jason Dominguez, Supervisory IT Cybersecurity Specialist
Rashedul Romel, IT Cybersecurity Specialist
Taurean McKenzie, IT Specialist
Jon Wyatt, System Administrator
Joseph Sanchez, IT Specialist

Data Services
Sandra Parsons, Assistant Inspector General, Office of Innovation
Johnson Joseph, Supervisory Data Analyst
Muhammad Islam, Statistician

Appendix D
Report Distribution

Department of Homeland Security

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

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