OFFICE OF INSPECTOR GENERAL

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

Homeland Security

September 7, 2022

OIG-22-65

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

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

September 7, 2022

MEMORANDUM FOR: The Honorable Ur M. Jaddou
Director
U.S. Citizenship and Immigration Services

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: 2022.09.07 08:22:08 -04'00'

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

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

The report contains ten recommendations aimed at improving USCIS access controls and departmental access control policies. Your offices concurred with all ten recommendations. Based on information provided in your response to the draft report, we consider all ten recommendations open and resolved. Once your offices have 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 of 1978, as amended,* 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 Bruce Miller, Deputy Inspector General for Audits, at (202) 981-6000.

DHS OIG HIGHLIGHTS

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

September 7, 2022

Why We Did This Audit

One of the most effective ways for an organization to reduce overall risk of cyberattacks is to ensure that only authorized users can access its networks, systems, and information. Access controls help to limit individuals from gaining inappropriate access to systems or data We conducted this audit to determine the extent to which USCIS is applying IT access controls to restrict unnecessary access to systems and information.

What We Recommend

We made 10 recommendations to improve USCIS' 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. Citizenship and Immigration Services (USCIS) did not apply the information technology (IT) access controls needed to restrict unnecessary access to its systems, networks, and information. USCIS did not consistently manage or remove access for its personnel once they departed positions and did not have a process to adequately verify access after personnel transferred offices within USCIS. Also, USCIS did not take all necessary steps to ensure privileged user access was appropriate and did not adequately manage and monitor service account access. These deficiencies stemmed from insufficient internal controls and day-to-day oversight to ensure access controls are administered appropriately and effectively to prevent unauthorized access.

Based on our testing, USCIS did not implement all the required security settings and updates for its IT systems and workstations to help reduce the impact if access control weaknesses are exploited. Although USCIS systems and workstations were generally compliant with required security standards, not all required settings and updates were implemented due to concerns that they may negatively impact system operations. Lastly, while USCIS appropriately relied on departmental guidance for access control policies and procedures, the guidance was outdated and did not include the latest Federal requirements.

USCIS is taking steps to enhance its access control and system security processes to address these deficiencies. Until fully addressed, these deficiencies may limit the Department's overall ability to reduce the risk of unauthorized access to its network, which may disrupt mission operations. Additionally, inadequate security settings on IT equipment may limit USCIS' capability to overcome a major cybersecurity incident.

DHS Response

DHS and USCIS concurred with all ten recommendations. We have included a copy of their comments in Appendix B.

Table of Contents

Appendixes

Abbreviations

AECO	Accountable Exit Clearance Officer
CISO	Chief Information Security Officer
DISA	Defense Information Security Agency
HCT	Human Capital and Training
ICAM	Identity Credential Access Management
IT	information technology
NIST	National Institute of Standards and Technology
OCIO	Office of Chief Information Officer
OIT	Office of Information Technology
STIG	Security Technical Implementation Guide
USCIS	U.S. Citizenship and Immigration Services

Background

Within the Department of Homeland Security, U.S. Citizenship and Immigration Services (USCIS) administers immigration benefits, including adjudicating petitions, applications, and requests for citizenship and lawful permanent residence, among others. During fiscal year 2020, USCIS processed 7.6 million applications, petitions, and requests. USCIS collects a significant amount of data from its applicants, including biometric and personally identifiable information, to help complete its mission. Over the past decade, USCIS has taken steps to digitize its vast inventory of immigration records to increase the efficiency and capacity of its workforce.

USCIS' mission makes its systems and networks a high visibility target by attackers seeking to steal sensitive information or disrupt immigration operations. Given the vast amount of data maintained by USCIS, implementing and maintaining appropriate information technology (IT) controls and settings across all accounts, devices, and IT systems is vital. One of the most effective ways to protect data, and reduce the risk of a cyberattack, is to enforce effective access controls for only appropriate users to have access to an organization's network, systems, and information. For example, effective access controls and system security would help to prevent a major cyberattack, such as the 2020 SolarWinds incident that resulted in senior DHS officials' email accounts being compromised. During the SolarWinds incident, attackers were believed to have breached cyber defenses by leveraging the software supply chain to gain access to Federal governments' networks.[1] Once inside the networks, attackers successfully set up permissions for themselves to access other programs and applications while being undetected. This type of cyber incident highlights the importance of maintaining and enforcing effective access controls.[2]

All executive branch agencies are required[3] to implement access controls as part of their security framework to help protect their operations and assets from threats, including hostile attacks, human errors, and foreign intelligence entities. The following access controls identified in Table 1 are best practices for Federal agencies:

[1] *Written Testimony of Sudhakar Ramakrishna, Chief Executive Officer, 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.
[2] *The SolarWinds Hackers Used Tactics Other Groups Will Copy,* Wired.com, January 19, 2021.
[3] OMB Circular A-130, *Managing Information as a Strategic Resource*, July 28, 2016.

Table 1. Overview of Access Control Phases

Access Control	Control Description
Initial Approval of Access	Individuals should formally submit requests for access and obtain explicit approval.
Access Removal	Individuals who no longer work for an organization should have their access removed immediately.
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., transfers job functions).
Least Privilege Access	This principle requires that each user in a system be granted the most restrictive set of privileges (or lowest clearance) needed to perform authorized tasks. It also limits the damage that can result from an accident, error, or unauthorized use.

Source: Office of Inspector General generated based on Federal, DHS, and USCIS criteria

USCIS' Administration of Technology and Access Control

USCIS Office of Information Technology (OIT) is responsible for providing adequate IT services and capabilities to enable USCIS performance. Within OIT, the Information Security Division is responsible for implementation of identity and access management security principles, IT security operations, and risk management programs. The Information Security Division has four branches, including the Identity Credential Access Management (ICAM) branch. ICAM is responsible for facilitating access control procedures throughout the component and for managing USCIS' official account and access management system, myAccess,[4] which has automated approval workflows to help ensure access requests are reviewed and approved by the appropriate individuals.

USCIS uses access controls to allow personnel to appropriately access its network and specific systems needed for performance of their mission duties. USCIS has established two primary types of IT user accounts: (1) regular and (2) privileged user accounts. USCIS must formally approve all account requests.

(1) Regular user accounts are provided to personnel who require basic access to USCIS information systems to perform mission duties. For example, a regular user account would be provided for an individual to check email.

(2) Privileged user accounts are used to perform security functions, such as system maintenance and configuration. For personnel responsible for performing IT security functions, USCIS provides both a privileged user account and a general user account. For example, a server

[4] myAccess was implemented in 2018 for system access requests and approvals.

administrator would use a privileged account to install system updates and a general user account to check email. Individuals should only use their privileged user account to perform elevated, security related duties. All other actions should be performed with their general user account.

USCIS uses general support systems[5] to provide technical capabilities and IT infrastructure to facilitate access controls and meet USCIS IT security requirements. USCIS IT infrastructure for supporting access controls includes the following general support systems:

- Enterprise Infrastructure Services 1: Provides core IT services such as Active Directory[6] and the infrastructure needed to support Active Directory.

- Identity Credential Access and Management System: Monitors when access is granted, refused, or inappropriately held open. The system consists of servers, control panels, and monitoring equipment.

- CISNet: Provides local computer equipment such as laptops, general file servers, backup devices, printers, and scanners at all USCIS sites within the United States processing immigration and naturalization data.

- Enterprise Hosting Services 1: Provides support for operating system, backup, database, and application security. In addition, USCIS Enterprise Hosting Services supports the continuity of operations through monitoring and alerting tools to manage the health and security of the infrastructure.

The SolarWinds cybersecurity incident of 2020 demonstrates the importance of implementing effective cybersecurity practices. We conducted this audit to determine the extent to which USCIS is applying IT access controls to restrict unnecessary access to systems and information.

Results of Audit

USCIS did not apply the IT access controls needed to restrict unnecessary access to its systems, networks, and information. USCIS did not consistently manage or remove access for its personnel once they departed positions within the agency and did not have a process to adequately verify access after

[5] An interconnected set of information resources under the same direct management control that shares common functionality. It normally includes hardware, software, information, data, applications, communications, and people.
[6] Active Directory stores information about user accounts, such as names, passwords, phone numbers, and enables other authorized users on the same network to access this information.

personnel transferred offices within USCIS. Also, USCIS did not take all necessary steps to ensure privileged user access was appropriate and did not adequately manage and monitor service account access. These deficiencies stemmed from insufficient internal controls and day-to-day oversight to ensure access controls are administered appropriately and effectively to prevent unauthorized access.

Our testing found that USCIS did not implement all the required security settings and updates for its IT systems and workstations to help reduce the impact if access control weaknesses are exploited. Although USCIS systems and workstations were generally compliant with required security standards, not all required settings and updates were implemented due to concerns that they may negatively impact system operations. Lastly, while USCIS appropriately relied on departmental guidance for access control policies and procedures, the guidance was outdated and did not include the latest Federal requirements.

USCIS is taking steps to enhance its access control and system security processes to address these deficiencies. Until fully addressed, these deficiencies may limit the Department's overall ability to reduce the risk of unauthorized access to its network, which may disrupt mission operations. Additionally, inadequate security settings on IT equipment may limit USCIS' capability to withstand a major cybersecurity incident.

USCIS Did Not Effectively Manage Access to Systems and Information

USCIS did not consistently manage or remove access for its personnel once they departed positions within the agency and did not have a process to adequately verify access after personnel transferred offices within USCIS. Also, USCIS did not take all necessary steps to ensure privileged user access was appropriate and did not adequately manage and monitor service account access. These deficiencies stemmed from insufficient internal controls and day-to-day oversight to ensure access controls are administered appropriately and effectively to prevent unauthorized access.

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

Removing access for separated personnel is the most effective method for ensuring that no former employees can access system resources after their term of employment has ended. DHS' IT security policy[7] requires that

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

separated and transferred[8] personnel who no longer require the same level of access have their IT access privileges terminated immediately. To implement DHS' requirement, USCIS aims to disable IT access within 24 hours of an individual's separation or transfer. According to its current policy,[9] USCIS requires that all system access be removed for individuals that separate from the component, and all system account access should be reviewed and removed as needed for individuals who transfer between USCIS offices.

USCIS Office of Human Capital and Training (HCT) implemented the Employee and Contractor Exit Clearance Process[10] to facilitate access reviews and removals for separated and transferred personnel. As part of this process, an individual's supervisor or contracting officer representative must notify the Accountable Exit Clearance Officer (AECO) of a separation or transfer to another USCIS program office. The process provides that personnel should notify the supervisor or contracting officer representative 2 weeks prior to the individual's separation or transfer date. Specifically,

- For separations, the AECO is responsible for generating a request to disable IT access in the ServiceNow ticketing system, including the date the access should be removed. This request is routed to the Service Desk for processing.

- For employees transferring to another USCIS office, the supervisor or Contracting Officer representative works with the receiving office to review all assigned system access and removing access that is no longer needed.

Separated Personnel

As part of this audit, we tested a statistical sample of all separated personnel from FY 2021. Even though access for separated personnel is required to be disabled immediately, we determined that 98 of 297 (33 percent) separated personnel had access to USCIS network beyond 24 hours of departure. Of the 98 separated personnel, 48 had access for at least 22 days after leaving. When properly notified of separating personnel through the Employee and Contractor Exit Clearance Process, the OIT Service Desk generally disabled accounts in a timely manner. For example, the OIT Service Desk either never received notification or received delayed or incorrect notification for 83 of the 98

[8] Personnel transfers occur when an individual moves from one USCIS office to a position in another USCIS office.
[9] USCIS Account Management Directive, 140-006.1, July 10, 2017.
[10] USCIS Management Directive 257-001.1, July 31, 2013.

personnel who were not disabled timely, causing access to remain active even though the individuals separated from USCIS.

This occurred because USCIS did not have adequate controls over the Employee and Contractor Exit Clearance Process. Instead of taking action to remove access for these individuals immediately after separation, USCIS relied on an automated control to disable access after 30 days of inactivity. USCIS HCT officials said that managers did not always notify the AECO of an individual's separation, preventing the account disablement request from being initiated and provided to the OIT Service Desk. Further, HCT officials stated they did not have an adequate process to identify managers who do not notify AECO of an individual's separation as required. HCT is developing a capability to identify unreported separations to help ensure that the AECO and the Service Desk are notified. HCT advised that the Employee and Contractor Exit Clearance Process has not been updated since 2013, but it is currently reviewing the process to make necessary changes to support access control management.

Transferred Personnel

USCIS did not monitor transferred employees to ensure their access was appropriate. Specifically, we identified 864 individuals who transferred USCIS offices during FY 2021 but were not formally tracked to verify their access was appropriate after changing offices. This occurred because HCT did not have controls in place to ensure that supervisors and Contracting Officer Representatives complied with the Employee and Contractor Exit Clearance Process. Although HCT generates a biweekly report identifying all transferred personnel, it did not use that report to verify that supervisors complied with transferred personnel requirements in the Employee and Contractor Exit Clearance Process.

The inconsistencies in the Employee and Contractor Exit Clearance Process meant that OIT could not implement automated settings to disable transferred personnel's access when it was not verified by the new supervisor. While USCIS automatically disables system access if other required policies have not been met, such as 30 days of inactivity, it did not have the data from the Employee and Contractor Exit Clearance Process to implement similar settings for transferred personnel. Instead, OIT relied on the transferred employee's new supervisor to proactively take action to review and verify access without additional controls to enforce USCIS requirements.

Officials acknowledged USCIS has not implemented a process to meet its requirement to review and remove access for individuals who transfer between USCIS offices. USCIS previously identified this issue during an internal security review in May 2017 and formally documented it as an item requiring remediation through the USCIS' Plan of Actions and Milestones Process.[11] USCIS' internal review determined that it lacked a process to notify OIT personnel of individuals transferring within USCIS which could result in uncertainty about an individual's access needs. USCIS planned to address this by May 4, 2022, but this was still outstanding as of August 2022.

USCIS Did Not Adequately Protect and Review Privileged User Access

USCIS' privileged users may be granted powerful access to sensitive assets and are trusted to perform critical IT security functions across USCIS' enterprise. Attackers often covet privileged accounts because of the broad access typically granted to these accounts to meet mission requirements. Accordingly, USCIS requires[12] that all account credentials used to logon to USCIS systems be protected and annual reviews of all privileged user accounts to help ensure that individuals are granted the most restrictive set of privileges needed to accomplish their mission.

Protecting Privileged User Access

We determined that USCIS did not adequately prevent privileged user account credentials from being exposed to potential attackers. USCIS personnel appropriately used their privileged account to perform maintenance on high value assets, such as enterprise support servers. However, we identified privileged users who were responsible for supporting USCIS' enterprise assets who were also granted local administrator access to workstations through their privileged account. By allowing this to occur, the credentials for privileged accounts with access to high value assets may be stored in workstation memory, allowing an attacker to extract this information from the less secure asset and use it to further their attacks and inappropriate access.[13]

This occurred because officials decided, due to mission requirements, not to restrict personnel from using the same privileged account to access both highly sensitive and less secure assets. Specifically, USCIS personnel only have one privileged account and require access to both sensitive (e.g., enterprise servers) and less secure assets (e.g., workstations) to perform their duties. Therefore, additional logon restrictions cannot be implemented to restrict access to their only privileged account without negatively impacting mission activities.

[11] Plans of Action and Milestones record and manage the mitigation and remediation of identified weaknesses and deficiencies.
[12] USCIS Account Management Directive, 140-006.1, July 10, 2017.
[13] Logon credentials may be saved to memory, allowing for this information to be extracted later.

USCIS was aware of this issue and was in the process of taking steps to address potential risks. In 2020, USCIS initiated a privileged account restructuring project to align USCIS account practices with the Microsoft Tiered Administrator Model. This model recommends that privileged accounts are issued to personnel based on the IT resources they will access and to provide personnel with multiple privileged accounts to access different types of assets. For example, if an individual needs to maintain both enterprise servers and workstations for his or her job function, the individual would be granted two separate privileged accounts: one to access the enterprise server and another to access the end user workstation. USCIS confirmed that under the new privileged account process, personnel will not be able to access highly sensitive and less secure assets from the same account. To complete its ongoing privileged account project, USCIS stated it must review and classify all USCIS assets, then assign new privileged accounts and associated permissions.

Privileged User Access Reviews

Although privileged users may be granted access to sensitive USCIS systems, we identified 599 individuals with privileged accounts who were responsible for performing IT security functions whose access was not reviewed annually, as required. These 599 privileged users included domain administrators, server administrators, and enterprise engineers who were not reviewed and recertified in the last year.[14] Moreover, 143 privileged users' access had not been formally reviewed in at least 9 years.

USCIS relies on the myAccess system to provide the data and automated workflow needed for supervisors to review and recertify user access annually. However, although myAccess has the capability to recertify access for general user accounts, it cannot recertify access for privileged administrator accounts. Without myAccess functionality, USCIS did not implement an alternative process to ensure privileged account recertification occurred as required. USCIS explained that myAccess was implemented in 2018 and that not all required functionalities could be added at initial deployment. USCIS plans to update myAccess in 2022 with a capability to recertify privileged user accounts.

USCIS Did Not Adequately Manage and Monitor Service Account Access

USCIS 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 since they are non-human accounts with

[14] Domain administrators support the engineering and operations on IT platforms, infrastructure, and engineering. Server administrators maintain applications on servers. Enterprise Engineers manage script modifications and group policy changes.

highly privileged access. USCIS requires service accounts to be reviewed annually, to restrict access to the minimum number of personnel with a mission need, and to prevent interactive logon.[15] Additionally, DHS requires for service account passwords be changed annually.

Annual Reviews of Service Account Access

Of the 112 service accounts we tested, 84 were not recertified in the last year, and 8 had not been recertified in over 5 years. Periodically reviewing service accounts is a key step in ensuring the accounts are still needed for mission purposes and have the minimum level of access needed to accomplish their function. USCIS did not review service accounts because the myAccess system did not have the capability to recertify service account access.

Restricting Service Account Access

USCIS did not consistently restrict unnecessary access to service accounts for users who did not have a mission need. Specifically, 61 users were allowed to reset the password to a highly privileged service account even though there was no mission need for access. By not restricting access to this service account, an attacker could compromise any of the 61 user accounts that had inappropriate access to impersonate legitimate activities and steal other account credentials. This occurred by error as USCIS stated the individuals inherited the permission to reset the service account passwords by mistake and that they were unaware this authorization had been granted.

Restricting Interactive Logon and Requiring Password Changes

Additionally, while USCIS prohibits individuals from using service accounts to interactively log into a system, we identified 738 service accounts that inappropriately permitted this access capability. When human users interactively log into service accounts, their identity cannot be easily monitored and service account permissions may be used without proper approval.

USCIS did not meet requirements to change passwords for service accounts. DHS has issued departmental guidance[16] requiring all service account passwords to be changed annually to help protect accounts from compromise. The longer a password exists, the higher the risk that the service account may be compromised by an attacker. Therefore, periodically changing passwords is important because they are often the first line of defense against intruders or

[15] Interactive logon is when a user accesses the account by providing credentials to access the account.
[16] Change Memorandum 13.1.1 to *DHS Sensitive Systems Policy Directive 4300A*, October 2, 2019.

insiders who may seek to obtain unauthorized access to a DHS system. However, we found 653 service accounts with passwords that had not been changed in over 1 year. In fact, 338 of these account passwords had not been changed for over 5 years.

USCIS did not appropriately restrict interactive logon to service accounts and change passwords as required due to its reliance on non-managed service accounts. Unlike managed service accounts, non-managed service accounts do not provide automatic password management or interactive logon restrictions. As a result of the non-managed service account limitations, USCIS could not efficiently manage account settings and therefore did not meet all DHS and USCIS policy requirements. Microsoft recommends the use of Managed Service Accounts[17] to restrict interactive logon and automatic password management.

USCIS Vulnerability Patch and Configuration Management of IT Infrastructure and Workstations

USCIS did not implement all the required security settings and updates for its IT systems and workstations to help reduce the impact if access control weaknesses are exploited. Although USCIS systems and workstations were generally compliant with required security standards, not all required settings and updates were implemented due to concerns that they might negatively impact system operations.

Vulnerability Patch Management

Vulnerability patch management programs are intended to increase security awareness and minimize risks to systems by helping to ensure effective and continuous identification, management, and tracking of risks and threats until they are addressed. USCIS is required to address vulnerabilities for its systems according to dates published through the DHS Enterprise Security Operations Center, Information Security Vulnerability Management notices.[18]

USCIS implemented a vulnerability patch management program, but the program did not adequately address weaknesses that were classified as critical and high-risk vulnerabilities.[19] Specifically, we identified critical and high-risk vulnerabilities that were not addressed within DHS' required timelines.[20] For example, we identified one USCIS system used for providing general system

[17] Managed Service Accounts do not allow for users to interactively logon.
[18] *DHS Sensitive Systems Policy Directive 4300A*, Version 13.1, July 27, 2017.
[19] The National Institute of Standards and Technology (NIST) has established the National Vulnerability Database Severity Ratings to evaluate the severity of weaknesses.
[20] Change Memorandum 13.1.1 to *DHS Sensitive Systems Policy Directive 4300A*, October 2, 2019.

support that had 8 unique critical vulnerabilities, with 27 critical vulnerability instances and 140 unique high vulnerabilities, with 2,070 high vulnerability instances. Further, we identified one unsupported operating system version for a Windows 10 workstation.

Although USCIS was aware of the vulnerability patch management deficiencies, it did not have software patch installation agents properly installed and a complete listing of all required patches.[21] USCIS has established working groups to actively resolve the vulnerability deficiencies and included these planned efforts in its FY 2022 strategic goals.

Configuration Management

Implementing configuration management standards is a key process used to apply and manage the settings needed for system security. According to *DHS Sensitive Systems Policy Directive* 4300A (Policy Directive 4300A), the Department requires components to follow technical setting frameworks, including the Defense Information Security Agency (DISA) *Security Technical Implementation Guides* (STIG).[22] DHS requires components to request a waiver to be exempted for the settings not implemented. However, USCIS did not implement all required DISA STIG settings and did not obtain an approved waiver for exemption. The four USCIS systems we tested were between 58 percent and 98 percent compliant with the DISA STIGs setting requirements.

According to USCIS officials, the configuration settings were not implemented due to concerns that the required settings might cause network and system disruptions. Although USCIS noted operational concerns and was aware of its noncompliance with the DISA STIG settings, it has not yet submitted or received approved waivers to bypass implementation requirements. According to USCIS officials, the agency plans to formally document the deficiencies in a Plan of Actions and Milestones and then obtain a waiver from the appropriate officials to accept the risk of settings not implemented.

DHS Has Not Updated Its Guidance for Access Controls

Although USCIS appropriately relied on departmental guidance for access control policies and procedures, the guidance was outdated and did not include the latest Federal requirements. DHS developed the Policy Directive 4300A and *DHS 4300A Sensitive Systems Handbook* (Handbook) to serve as the Department's information security framework for components, including

[21] Patch management is the process of identifying, installing, and verifying code revision updates for applications software.
[22] The DISA STIGs contain technical guidance and standards to secure information system/software that might otherwise be vulnerable to a malicious computer attack.

USCIS.[23] However, the Policy Directive 4300A and Handbook did not include the latest requirements mandated by the National Institute of Standards and Technology (NIST) Publication 800-53, *Security and Privacy Controls for Information Systems and Organizations*, Revision 5 (NIST 800-53 Revision 5).[24]

The DHS Office of the Chief Information Officer (OCIO) is responsible for updating the Policy Directive 4300A and Handbook annually, and as required, when security standards such as NIST 800-53 change. However, DHS did not update the Policy Directive 4300A and Handbook. Namely, the Office of Management and Budget required all legacy IT systems to implement September 2020 requirements provided in NIST 800-53, Revision 5 by September 23, 2021.[25] As of March 2022, DHS had not implemented these requirements.

We identified at least 88 access control changes or additions in the latest version of NIST 800-53 Revision 5 that may require updates to Policy Directive 4300A. DHS Office of the Chief Information Security Officer[26] (CISO) is updating *DHS Sensitive Systems Policy Directive 4300A* to ensure it includes NIST 800-53 Revision 5 requirements. Specifically, the updated directive will be organized by control family and include DHS organizationally defined values for security requirements. Additionally, DHS CISO is streamlining to help make the directive easier to implement, update, and audit.

DHS OCIO did not have a standardized change management process for identifying and implementing required changes. As of April 2022, DHS CISO drafted a timeline anticipating the directive would be finalized by September 30, 2022.

Conclusion

Without effective access controls to review, remove, and manage personnel's access to its systems, USCIS is at increased risk of unauthorized individuals gaining access to sensitive information. USCIS collection of sensitive data for immigration benefit processing and its recent efforts to digitize this information for electronic use make it a high visibility target for attackers. Additionally, USCIS' access control deficiencies increase its attack surface and potential avenues for malicious actors to initiate a cyberattack. USCIS' inadequate security settings on systems and workstations may limit its capability to overcome an access control weakness if an unauthorized individual gains

[23] *DHS Sensitive Systems Policy Directive 4300A*, Version 13.1, July 27, 2017.
[24] NIST Special Publication 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, September 2020.
[25] OMB Circular A-130, *Managing Information as a Strategic Resource*, July 28, 2016.
[26] DHS Office of the Chief Information Security Officer is a component of the DHS Office of the Chief Information Officer.

access. DHS' security posture relies on all components to implement effective IT security processes; therefore, USCIS' access control and system security setting deficiencies may limit the Department's ability to reduce the risk of unauthorized access to its network and disrupting mission operations.

Recommendations

Recommendation 1: 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.

Recommendation 2: 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.

Recommendation 3: 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.

Recommendation 4: 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.

Recommendation 5: 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.

Recommendation 6: 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.

Recommendation 7: We recommend the Office of Information Technology finalize and implement patching procedures for assessing and resolving system vulnerabilities.

Recommendation 8: We recommend the Office of Information Technology implement all required DISA STIG configuration settings for Enterprise Hosting Services, Enterprise Infrastructure Services, and Identity Credential Access and Management and Citizenship and Immigration Services Network or request a waiver to exclude settings that cannot be implemented.

Recommendation 9: We recommend the DHS Chief Information Officer update the DHS 4300A Policy Directive and Handbook with the access control updates required by NIST 800-53, Revision 5.

Recommendation 10: 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.

Management Comments and OIG Analysis

We obtained written comments on a draft of this report from USCIS and the DHS OCIO through the Director of the Departmental GAO-OIG Liaison Office. In the comments, the Department indicated it appreciated our work on this audit. The Department stated that it remains committed to sustaining a strong Information Security Program that effectively protects data and information systems, while supporting DHS' mission of protecting the American people from threats to their security.

We have reviewed USCIS and DHS OCIO comments, as well as the technical comments previously submitted under separate cover, and updated the report as appropriate. Ten recommendations are open and resolved. A summary of the USCIS and DHS OCIO's responses and our analysis follows.

DHS Response to Recommendation #1: Concur. USCIS HCT is currently in the process of updating the Exit Clearance Process. Specifically, HCT's Human Resources Information Technology division is collaborating with USCIS OIT to compare the "Movement Reports" (such as Federal Losses, Internal Movement, and Contractor Separations) with electronic Exit Clearance requests on the myIT system. Once this update is complete, automated emails will be sent to supervisors and/or Contracting Officer's Representatives for missing myIT exit requests, as appropriate.

USCIS HCT's Employee Programs and WorkLife Services Division, in coordination with the OIT Audit Manager, will evaluate the current Employee and Contractor Exit Clearance process to ensure timelines are clearly defined for the removal of access.

Further, USCIS HCT's Employee Programs and WorkLife Services Division published the first of a series of quarterly articles on February 28, 2022, which reminded management, Accountable Exit Clearance Officers, and Contracting Officer's Representatives of the importance of Exit Clearance requirements, and

HCT will also begin offering quarterly trainings for management officials, AECOs and CORs in October 2022 to discuss Exit Clearance requirements for separated employees and contractors. In addition, by August 30, 2023, HCT will provide a draft of a revised Management Directive, 257-001.1, "Employee and Contractor Exit Clearance Process," and request that stakeholders provide feedback on any additional process or automation updates needed, as appropriate.

OIG Analysis: USCIS' actions are responsive to this recommendation, which will remain open and resolved until it provides documentation showing that the new Employee and Contractor Exit Clearance process, policy, and trainings have been enhanced and are operating as intended. USCIS estimates a completion date of December 29, 2023.

DHS Response to Recommendation #2: Concur. USCIS OIT and HCT will work collaboratively, along with other stakeholders, as appropriate to define: (1) transfer types; (2) what access is required; and (3) when mandatory access review is needed, as well as to best make available the process for reviewing and verifying the access of transferees (or a waiver).

OIG Analysis: USCIS' actions are responsive to this recommendation, which will remain open and resolved until it provides documentation showing that it has defined personnel transfer types and that access reviews are completed for these individuals as required by DHS policy. USCIS estimates a completion date of December 29, 2023.

DHS Response to Recommendation #3: Concur. Currently all non-privileged accounts are recertified via myAccess. As of April 2022, USCIS Identity Credential Access Management (ICAM) branch was able to validate the recertification of all 737 privileged accounts, and will establish a process to enforce recertification annually going forward. Similarly, service account recertification will be completed during fiscal year (FY) 2023. USCIS ICAM will continue working to integrate accounts into myAccess, ensuring the automated enforcement of annual recertification for non-privileged, privileged and service accounts.

OIG Analysis: USCIS' actions are responsive to this recommendation, which will remain open and resolved until it provides documentation showing myAccess functionality for validating privileged and service accounts annually and that the account validations are being completed as required. USCIS estimates a completion date of March 31, 2023.

DHS Response to Recommendation #4: Concur. USCIS OIT is developing a role-based access control model for all privileged accounts. Once complete, users will have access to assets based on the privileged roles assigned as a part of the new tiered account structure, and roles will be defined based on responsibilities within specific job functions. Accordingly, privileged roles will contain the minimum permissions required to perform assigned privileged tasks.

OIG Analysis: USCIS' actions are responsive to this recommendation, which will remain open and resolved until it implements the new role-based access control model for privileged user accounts. USCIS estimates a completion date of March 31, 2023.

DHS Response to Recommendation #5: Concur. Managed service accounts are currently used at USCIS when operationally appropriate and feasible. However, due to operational constraints, this cannot be implemented for all service accounts. For example, managed service accounts are typically implemented for accounts managed via Active Directory, but all of USCIS accounts are not managed via Active Directory. Therefore, implementation of managed service accounts for non-Active Directory accounts would introduce significant financial burden. As a part of the myAccess recertification process that USCIS ICAM will complete during FY 2023, service account owners will be notified annually of requirements to reset service account passwords. ICAM will also conduct additional analysis to determine what actions are necessary to ensure that service account owners take action to reset service account passwords in a timely manner, as appropriate.

OIG Analysis: USCIS' actions are responsive to this recommendation, which will remain open and resolved until USCIS implements its myAccess recertification process and completes its analysis of what actions are necessary to ensure service account owners reset passwords as required. We understand financial and operational limitations may prevent managed service accounts from being fully implemented for all accounts. USCIS estimates a completion date of June 30, 2023.

DHS Response to Recommendation #6: Concur. USCIS OIT will perform an analysis against existing service accounts to determine the appropriate owners, as well as the purpose of each account. Upon completion of this review, OIT will consider which privileges qualify for removal.

OIG Analysis: USCIS' actions are responsive to this recommendation, which will remain open and resolved until it provides documentation detailing the methodology and results of the service account analysis. USCIS estimates a completion date of June 30, 2023.

DHS Response to Recommendation #7: Concur. USCIS OIT established a Vulnerability Management Team on December 13, 2021, to improve its Vulnerability Management process by coordinating vulnerability remediation and patching efforts between various teams across the enterprise. This project is aimed at identifying significant gaps that exist within the current process. As OIT establishes an improved process, prioritization and coordination of patching and remediation efforts will be considered, as appropriate.

OIG Analysis: USCIS' actions are responsive to this recommendation, which will remain open and resolved until the Vulnerability Management Team completes its project for identifying significant gaps and the prioritization, coordination, and remediation of vulnerabilities as appropriate. USCIS estimates a completion date of March 31, 2023.

DHS Response to Recommendation #8: Concur. USCIS OIT is currently developing a formalized set of processes and procedures to effectively develop, manage, maintain, and deploy STIG compliant operating system baseline images to improve Configuration Management process. Additionally, USCIS OIT's Weakness Remediation Manager will implement processes and procedures to ensure that all configurable assets are associated with approved benchmarks if STIGs are not available, as well as run configuration scans on all systems. The Plan of Action & Milestones and waiver process will be used to document any settings that cannot be implemented.

OIG Analysis: USCIS' actions are responsive to this recommendation, which will remain open and resolved until it provides the updated policies and procedures related to STIG compliance and configuration management improvements, to include the configuration scan results and Plan of Action & Milestones for settings that cannot be implemented. USCIS estimates a completion date of June 30, 2023.

DHS Response to Recommendation #9: Concur. DHS OCIO is currently in the process of updating DHS Policy Directive 4300A, "Sensitive Systems Handbook," dated November 15, 2015, to streamline existing policy and guidance attachments to make implementing, auditing, and updating easier.

During FY 2021, progress on this update and integration of new policies with the revision of existing policies in 4300A slowed due to a variety of exigent operational requirements. For example, DHS was primarily focused on responding to a significant cyber incident in FY 2021, as the Department resources were diverted for critical SolarWinds response and recovery efforts.

However, the DHS Office Chief Information Security Officer is: (1) simplifying the 4300A policy process and procedures; (2) eliminating the

Sensitive Systems Handbook; (3) shortening the underlying document from several hundred pages to fewer than 100 pages; and (4) socializing the updated policies with the Chief Information Security Officer and Chief Executive Officer communities. This effort will culminate in a full update of DHS 4300A and all dependent policies, by the end of FY 2022

OIG Analysis: DHS' actions are responsive to this recommendation, which will remain open and resolved until it finalizes the updates to 4300A processes and issues the updated policy directive. DHS OCIO estimates a completion date of September 30, 2022.

DHS Response to Recommendation #10: Concur. DHS Office Chief Information Security Officer, within the OCIO, is also updating the 4300A policy to formalize the change management process. Once complete, the new process will include the review and approval of all 4300A policy change requests by the DHS CISO Council that is led by the DHS CISO.

OIG Analysis: DHS' actions are responsive to this recommendation, which will remain open and resolved until it provides an updated policy formalizing the change management process. DHS OCIO estimates a completion date of September 30, 2022.

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 USCIS is applying IT access controls to restrict unnecessary access to systems and information. We evaluated USCIS' account management processes for authorizing, validating, and disabling users' access. Additionally, we performed technical assessments of USCIS domain and selected systems to identify weaknesses and security risks.

To conduct this audit, we gathered system documentation related to access control implementation and evidence of access control related actions for user account creation, disablement, and validation. We also obtained data from the Office of Human Capital and Training to identify personnel that separated or transferred offices and should have been subject to access requirement changes. Additionally, we observed systems to understand USCIS account management processes for account creation, disablement, and removal. We conducted interviews with the USCIS Identity and Credential Access Management Branch, Information Security Division, Service Desk Operations, Human Resource Information Technology Division, system owners, and information system security officers. We also interviewed the DHS Office of the Chief Information Officer. We researched and used Federal and departmental criteria for access control requirements.

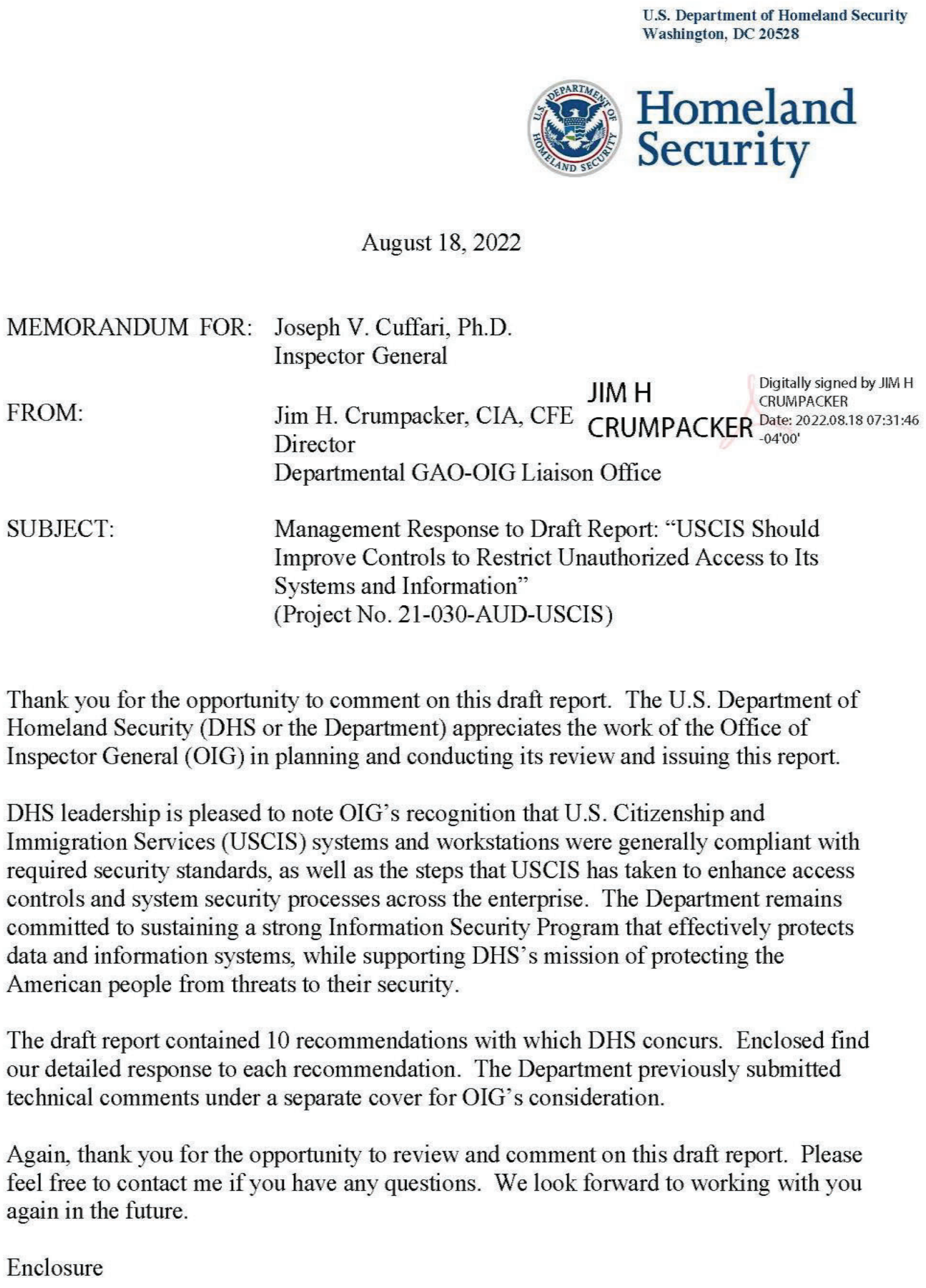
Additionally, we relied on the work of internal specialists from the OIG's Office of Innovation, Cybersecurity Risk Assessment Division to perform technical assessments of USCIS systems and domain. Their work included patch and configuration management assessments on servers with selected systems and a statistically valid sample size of workstations. The internal specialists also completed an active directory assessment scan of the USCIS network. The information obtained from the scans was used to identify weaknesses such as missing security patches, misconfigured security settings, presence of unsupported operating systems, and Active Directory weaknesses or misconfigurations.

To ensure the accuracy of testing results and OIG reporting, USCIS was given the opportunity to review preliminary observations from testing to verify initial testing results and to identify "false-positive" results. We reviewed USCIS feedback and updated our analysis as needed. Additionally, when writing the report, the OIG considered the potential for sensitivity issues under DHS

Management Directive 11042.1, Safeguarding Sensitive But Unclassified Information, and generalized findings as appropriate to avoid disclosing information designated as sensitive by the Department. The OIG further obtained verification from DHS headquarters and USCIS OIT officials that the report was reviewed for sensitivity concerns.

We conducted this performance audit between May 2021 and February 2022 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 upon our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based upon our audit objectives.

Appendix B
DHS Comments to the Draft Report



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

Homeland Security

August 18, 2022

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

FROM: Jim H. Crumpacker, CIA, CFE
Director
Departmental GAO-OIG Liaison Office

JIM H CRUMPACKER
Digitally signed by JIM H CRUMPACKER
Date: 2022.08.18 07:31:46 -04'00'

SUBJECT: Management Response to Draft Report: "USCIS Should Improve Controls to Restrict Unauthorized Access to Its Systems and Information"
(Project No. 21-030-AUD-USCIS)

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

DHS leadership is pleased to note OIG's recognition that U.S. Citizenship and Immigration Services (USCIS) systems and workstations were generally compliant with required security standards, as well as the steps that USCIS has taken to enhance access controls and system security processes across the enterprise. The Department remains committed to sustaining a strong Information Security Program that effectively protects data and information systems, while supporting DHS's mission of protecting the American people from threats to their security.

The draft report contained 10 recommendations with which DHS concurs. Enclosed find our detailed response to each recommendation. The Department previously submitted technical comments 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 21-030-AUD-USCIS

OIG recommended the USCIS Office of Human Capital and Training (HCT) in conjunction with the USCIS Office of Information Technology (OIT):

Recommendation 1: Evaluate the Employee and Contractor Exit Clearance Process and update it 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.

Response: Concur. USCIS HCT is currently in the process of updating the Exit Clearance Process. Specifically, HCT's Human Resources Information Technology division is collaborating with USCIS OIT to compare the "Movement Reports" (such as Federal Losses, Internal Movement, and Contractor Separations) with electronic Exit Clearance requests on the myIT system. Once this update is complete, automated emails will be sent to supervisors and/or Contracting Officer's Representatives (CORs) for missing myIT exit requests, as appropriate. An official personnel action is the mechanism that prompts separation or transfer and facilitates appropriate system updates, and is reflected in the separation report from the National Finance Center, which occurs at least 3 weeks after the personnel action is processed.

Specifically, USCIS HCT's Employee Programs and WorkLife Services Division, in coordination with the OIT Audit Manager, will evaluate the current Employee and Contractor Exit Clearance process to ensure timelines are clearly defined for the removal of access. Automation will also be considered as OIT and HCT work together to develop a solution to consistently identify and disable access in accordance with DHS policy and USCIS policy.

Further, USCIS HCT's Employee Programs and WorkLife Services Division published the first of a series of quarterly articles on February 28, 2022, which reminded management, Accountable Exit Clearance Officers (AECOs), and CORs of the importance of Exit Clearance requirements, and HCT will also begin offering quarterly trainings for management officials, AECOs and CORs in October 2022 to discuss Exit Clearance requirements for separated employees and contractors. In addition, by August 30, 2023, HCT will provide a draft of a revised Management Directive, 257-001.1, "Employee and Contractor Exit Clearance Process,"[1] and request that stakeholders provide feedback on any additional process or automation updates needed, as appropriate.

[1] https://connect.uscis.dhs.gov/org/EXSO/Management Directives/257-001.1.pdf

The updates to the Exit Clearance process requires collaboration between OIT, HCT, the Office of Security and Integrity (OSI), and Contracting to develop and implement a process that provides the necessary controls around identifying and communicating separated employees. In a collaborative effort, HCT and OIT will develop a project schedule to include key milestones and milestone dates for updating the USCIS Employee and Contractor Exit Clearance process. The completion of the planned work is dependent upon the potential identification of acquisition needs, IT systems integrations, development of new processes, and training needs. Estimated Completion Date (ECD): December 29, 2023.

Recommendation 2: 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.

Response: Concur. USCIS OIT and HCT understand the critical need to establish a process to fulfill the intent of this recommendation. Although USCIS Human Resources track various personnel actions such as internal transfers, the bi-weekly Internal Movement Reports do not trigger an IT account review of privileges. Currently, accounts are reviewed at least annually to ensure users retain only necessary privileges.

HCT and OIT will work collaboratively, along with other stakeholders as appropriate, to define: (1) transfer types; (2) what access is required; and (3) when mandatory access review is needed, as well as to best make available the process for reviewing and verifying the access of transferees (or a waiver). However, it is important to note that the aforementioned updates requires extensive collaboration between OIT, HCT, OSI, and Contracting to develop and implement a process that provides the necessary controls around transferred employees and contracts. Specifically, HCT and OIT will develop a project schedule to include key milestones and milestone dates for updating the process for identifying transferred employees, and the estimated completion date provided in this response is tentative and may require adjustment once HCT and other stakeholders have clearly defined the processes and the necessary automated systems need to manage transferred users. ECD: December 29, 2023.

OIG recommended the USCIS OIT:

Recommendation 3: Develops and implements 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.

Response: Concur. Currently all non-privileged accounts are recertified via myAccess. As of April 2022, USCIS Identity Credential Access Management (ICAM) branch was able to validate the recertification of all 737 privileged accounts, and will establish a process to enforce recertification annually going forward. Similarly, service account recertification will be completed during fiscal year (FY) 2023. USCIS ICAM will continue working to integrate accounts into myAccess, ensuring the automated enforcement of annual recertification for non-privileged, privileged and service accounts. ECD: March 31, 2023.

Recommendation 4: Finalize implementation of the proposed tiered privileged account project that allows users to use separate accounts when accessing less secure assets.

Response: Concur. OIT is currently in the process developing a Role Based Access Control model for all privileged accounts. Once complete, users will have access to assets based on the privileged roles assigned as a part of the new tiered account structure, and roles will be defined based on responsibilities within specific job functions. Accordingly, privileged roles will contain the minimum permissions required to perform assigned privileged tasks. ECD: March 31, 2023.

Recommendation 5: Implement managed service accounts or additional manual/technical controls to deny interactive logon and reset service account passwords timely.

Response: Concur. Managed service accounts are currently used at USCIS when operationally appropriate and feasible. However, due to operational constraints, this cannot be implemented for all service accounts. For example, managed service accounts are typically implemented for accounts managed via Active Directory, but all of USCIS accounts are not managed via Active Directory. Therefore, implementation of managed service accounts for non-Active Directory accounts would introduce significant financial burden and require the implementation of alternative account management solutions for accounts not compatible with Active Directory. As a part of the myAccess recertification process that USCIS ICAM will complete during FY 2023, service account owners will be notified annually of requirements to reset service account passwords. ICAM will also conduct additional analysis to determine what actions are necessary to ensure that service account owners take action to reset service account passwords in a timely manner, as appropriate. ECD: June 30, 2023.

Recommendation 6: Perform an evaluation of Active Directory configurations based on users' roles and responsibilities and remove unnecessary privileges that allow access to service accounts.

Response: Concur. USCIS OIT will perform an analysis against existing service accounts to determine the appropriate owners, as well as the purpose of each account. Upon completion of this review, OIT will consider which privileges qualify for removal. ECD: June 30, 2023.

Recommendation 7: Finalize and implement patching procedures for assessing and resolving system vulnerabilities.

Response: Concur. USCIS OIT established a Vulnerability Management Team on December 13, 2021, to improve its Vulnerability Management process by coordinating vulnerability remediation and patching efforts between various teams across the enterprise. This project is aimed at identifying significant gaps that exist within the current process. As OIT establishes an improved process, prioritization and coordination of patching and remediation efforts will be considered, as appropriate. ECD: March 31, 2023.

Recommendation 8: Implement all required DISA [Defense Information Security Agency] STIG [Security Technical Implementation Guides] configuration settings for Enterprise Hosting Services, Enterprise Infrastructure Services, and the Identity Credential Access and Management and Citizenship and Immigration Services Network, or request a waiver to exclude settings that cannot be implemented.

Response: Concur. USCIS OIT is currently developing a formalized set of processes and procedures to effectively develop, manage, maintain, and deploy STIG-Compliant Operating System baseline images to improve Configuration Management process. Additionally, USCIS OIT's Weakness Remediation Manager will implement processes and procedures to ensure that all configurable assets are associated with approved benchmarks if STIGs are not available, as well as run configuration scans all systems. The Plan of Action & Milestones and waiver process will be used to document any settings that cannot be implemented. ECD: June 30, 2023.

OIG recommended the DHS Chief Information Officer:

Recommendation 9: Update Policy Directive 4300A and the related Handbook with the access control updates required by NIST [National Institute of Standard and Technology] 800-53, Revision 5.

Response: Concur. DHS OCIO is currently in the process of updating DHS Policy Directive 4300A, "Sensitive Systems Handbook," dated November 15, 2015,[2] to streamline existing policy and guidance attachments to make implementing, auditing, and updating easier. Specific improvements will include:

- Incorporating recently updated Federal Policies and Directives.
- Developing Organizationally Defined Values specific to DHS.
- Aligning controls with guidance provided by the following NIST Special Publications (SP):

[2] https://www.dhs.gov/publication/dhs-4300a-sensitive-systems-handbook

  - SP 800-53, "Security and Privacy Controls for Information Systems and Organizations," dated October 2020;[3]
  - SP 800-37, "Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy," dated December 2018;[4]
  - SP 800-171, "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations," dated January 2021;[5] and
  - SP 800-161, "Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations," dated May 2022.[6]
- Modularizing policy guidance to incorporate linkages to approved Enterprise requirements, processes, standards, and guidelines.

During FY 2021, progress on this update and integration of new policies with the revision of existing policies in 4300A slowed due to a variety of exigent operational requirements. For example, DHS was primarily focused on responding to a significant cyber incident in FY 2021, as the Department resources were diverted for critical SolarWinds response and recovery efforts.

However, the DHS Office Chief Information Security Officer (OCISO) is: (1) simplifying the 4300A policy process and procedures; (2) eliminating the Sensitive Systems Handbook; (3) shortening the underlying document from several hundred pages to fewer than 100 pages; and (4) socializing the updated policies with the Chief Information Security Officer (CISO) and Chief Executive Officer communities. This effort will culminate in a full update of DHS 4300A and all dependent policies, by the end of FY 2022. ECD: September 30, 2022.

Recommendation 10: Develop a formalized change management process to identify and implement Policy Directive 4300A updates as governing policies and standards require.

Response: Concur. DHS OCISO, within the OCIO, is also updating the 4300A policy to formalize the change management process. Once complete, the new process will include the review and approval of all 4300A policy change requests by the DHS CISO Council that is led by the DHS CISO. ECD: September 30, 2022.

[3] https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final
[4] https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final
[5] https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final
[6] https://csrc.nist.gov/publications/detail/sp/800-161/rev-1/final

Appendix C
Office of Audits Major Contributors to This Report

Tarsha Cary, Director
Alexander Stewart, Audit Manager
Kenneth Schoonover, Auditor-in-Charge
Stephanie Matthews, Auditor
Tessa Clement, Program Analyst
Alexandria Castaneda, Program Analyst
Donna Zavesky, Auditor
Charles Twitty, Supervisory Auditor
Lindsay Koch, Communications Analyst

Office of Innovation, IT and Data Specialist Support

Cybersecurity Risk Assessment
Thomas Rohrback, Director
Jason Dominguez, Supervisory IT Cybersecurity Specialist
Rashedul Romel, Supervisory IT Cybersecurity Specialist
Taurean McKenzie, IT Specialist
Jon Wyatt, IT Cybersecurity Specialist/System Administrator
Jerel Morton, OIG Contractor
Steve Wilson, OIG Contractor

Data Architecture and Engineering
Josh Wilshere, Supervisory Data Architect
Nandini Parvathareddygari, Senior Data Architect

Appendix D
Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
Chief 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
Respective Component Head, if not the Addressee
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" tab. If you cannot access our website, call our hotline at (800) 323-8603, fax our hotline at (202) 254-4297, 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