OFFICE OF INSPECTOR GENERAL

DHS Did Not Always Promptly Revoke PIV Card Access and Withdraw Security Clearances for Separated Individuals

Homeland Security

December 20, 2022
OIG-23-04

OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

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

December 20, 2022

MEMORANDUM FOR: Randolph D. Alles
Senior Official Performing the Duties of the Under
Secretary for Management
Department of Homeland Security

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

JOSEPH V CUFFARI
Digitally signed by JOSEPH V CUFFARI
Date: 2022.12.20 11:00:14 -05'00'

SUBJECT: *DHS Did Not Always Promptly Revoke PIV Card Access and Withdraw Security Clearances for Separated Individuals*

Attached for your action is our final report, *DHS Did Not Always Promptly Revoke PIV Card Access and Withdraw Security Clearances for Separated Individuals.* We incorporated the formal comments provided by your office.

The report contains six recommendations to improve the Department's controls over separated individuals' personal identity verification (PIV) card access and security clearances. Your office concurred with the six recommendations. Based on information provided in your response to the draft report, we consider recommendations one through six open and resolved. Once your office has fully implemented the recommendations, please submit a formal closeout letter to OIGAuditsFollowup@oig.dhs.gov within 30 days so that we may close the recommendations. The memorandum should be accompanied by evidence of completion of agreed-upon corrective actions.

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.

Attachment

DHS OIG HIGHLIGHTS

DHS Did Not Always Promptly Revoke PIV Card Access and Withdraw Security Clearances for Separated Individuals

December 20, 2022

Why We Did This Audit

DHS uses PIV cards and security clearances to control access to its systems and facilities. Our objective was to determine whether DHS terminated PIV card access and security clearances for separated employees and contractors in accordance with Federal regulations and Department policies.

What We Recommend

This report contains six recommendations aimed at improving DHS' controls over separated individuals' PIV card access and security clearances.

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

The Department of Homeland Security did not always terminate personal identity verification (PIV) card access or withdraw security clearances for separated employees and contractors in accordance with Federal regulations and Department policies. In 2018, we identified weaknesses in DHS' controls over PIV card collection, revocation, destruction, and management oversight. Many of the issues we previously reported remain, and further work is required to improve and enhance processes. Specifically, DHS has not prioritized ensuring that PIV cards are terminated when individuals no longer require access.

We determined that, in thousands of cases, DHS did not promptly revoke PIV card access privileges or destroy PIV cards of individuals who separated from the Department. In addition, DHS did not always promptly withdraw security clearances of individuals who separated from DHS. Unfortunately, we could not determine the exact magnitude of the problem because records in DHS' information systems were incomplete.

These issues occurred because DHS did not effectively manage and monitor its electronic systems of record or ensure DHS officials followed offboarding processes. Without effective PIV card and security clearance management and monitoring, DHS cannot ensure only authorized employees and contractors have access to its controlled systems and facilities.

DHS Response

DHS concurred with all six recommendations. We consider them open and resolved.

Background

In 2004, the President issued Homeland Security Presidential Directive-12 (HSPD-12), *Policies for a Common Identification Standard for Federal Employees and Contractors*. HSPD-12 requires Federal agencies to enhance security by issuing a government-wide, secure, and reliable form of identification.[1] To implement HSPD-12, the National Institute of Standards and Technology (NIST) established the personal identity verification (PIV) card as the common form of identification across the Federal Government.[2] The Department of Homeland Security issues PIV cards to individuals who need access to networks and information systems or physical access to DHS sites and facilities. The Department considers PIV cards, which can remain active for up to 6 years, sensitive and high-value items with "grave potential for misuse if lost, stolen, or compromised."[3]

Each PIV card includes a photo of the cardholder and lists the sponsoring agency, the cardholder's name, and an expiration date. Each card also has an embedded chip with certificates and keys to verify the authenticity of the card, which allows cardholders to access secured areas and information systems. DHS uses the Identity Management System (IDMS) as its system of record to store information on an individual's organization, affiliation, credentials, and PIV card history and status. The *DHS PCI Operations Plan*[4] defines roles and responsibilities related to the PIV card process. The plan requires DHS to prevent separated individuals from continuing to access Department systems and facilities. When cardholders separate from a DHS position, security officials must collect, revoke, and destroy their PIV cards. During this process, security officials must also update IDMS to reflect the status of PIV cards and maintain accountability for their locations.

DHS uses security clearance determinations to grant personnel access to the appropriate levels of information, systems, and facilities they need to perform their work. DHS refers to this level of access as "need to know." In accordance with Part 1400 of Title 5 of the Code of Federal Regulations, all positions must be evaluated for a position sensitivity designation commensurate with the position's responsibilities and assignments as they relate to the impact on

[1] The DHS Office of the Chief Security Officer (OCSO) is responsible for administratively implementing HSPD-12 requirements, including program planning, operations, business management, communications, and technical strategy.

[2] HSPD-12 requires "the Secretary of Commerce [to] promulgate in accordance with applicable law a Federal standard for secure and reliable forms of identification." NIST is a part of the Department of Commerce. Federal Information Processing Standard 201-02, *Personal Identity Verification of Federal Employees and Contractors,* issued August 2013, was the version in effect during our audit.

[3] *DHS Authorized Authoritative Credential Holder Responsibility Agreement*, Version 5.1, December 2021.

[4] *DHS PCI Operations Plan*, Version 5.0, issued December 23, 2016. PCI stands for PIV card issuer.

national security. The position description sensitivity level establishes the level of access necessary for a specific role.

DHS uses the Integrated Security Management System (ISMS) as its system of record to manage and process personnel security–related clearance actions and eligibility for access to information, positions, and assignments. When an individual separates from a DHS position,[5] responsible DHS officials must deactivate or administratively withdraw the accompanying security clearance in ISMS. DHS Instruction 121-01-007-01[6] defines roles and responsibilities related to the security clearance withdrawal process.

Previously Reported Challenges

In 2018, the DHS Office of Inspector General identified weaknesses in DHS' controls over PIV card collection, revocation, destruction, and management oversight.[7] In that audit, we determined that unauthorized individuals could gain access to Department facilities because DHS did not promptly collect, and revoke separated individuals' PIV cards. We recommended DHS develop and implement a process to collect, revoke, and destroy PIV cards for all contractors who no longer required access to DHS facilities or systems. In response to the recommendation, DHS created the Access Lifecycle Management (ALM) system to automate, streamline, centralize, and manage identity-based access rights for DHS employees and contractors.[8]

Results of Audit

DHS did not always terminate PIV card access and withdraw security clearances for separated employees and contractors in accordance with Federal regulations and Department policies. Many of the issues we previously reported remain unresolved. Specifically, DHS has not prioritized ensuring that PIV cards are terminated when individuals no longer require access. We determined that, in thousands of cases, DHS did not promptly revoke PIV card access privileges or destroy PIV cards of individuals who separated from the

[5] An individual may separate because of a failed background check, detail or contract completion or cancellation, transfer, retirement, resignation, termination, or death, thereby revoking their "need to know."

[6] DHS Instruction 121-01-007-01, *The Department of Homeland Security Personnel Security, Suitability and Fitness Program*, Revision 01, issued August 8, 2016, and updated June 14, 2017.

[7] *Department-wide Management of the HSPD-12 Program Needs Improvement*, OIG-18-51, February 14, 2018, https://www.oig.dhs.gov/sites/default/files/assets/2018-02/OIG-18-51-Feb18.pdf.

[8] ALM is currently operational at DHS Headquarters (HQ), the Federal Emergency Management Agency, and U.S. Immigration and Customs Enforcement. DHS planned to complete implementation of ALM throughout the Department from fiscal years 2018 through 2021. However, DHS has not met this milestone.

Department. In addition, DHS did not always promptly withdraw security clearances of individuals who separated from DHS. Unfortunately, we could not determine the exact magnitude of the problem because records in DHS' information systems were incomplete.

These issues occurred because DHS did not effectively manage and monitor IDMS and ISMS or ensure DHS officials followed offboarding processes. Without effective PIV card and security clearance management and monitoring, DHS cannot ensure only authorized individuals have access to its controlled electronic systems and facilities.

DHS Did Not Always Revoke Access for Separated Individuals

DHS Did Not Always Revoke PIV Cards

DHS requires that individuals have their access privileges terminated (i.e., revoked) immediately after separating from the Department.[9] This is consistent with Office of Management and Budget (OMB) guidance[10] to revoke PIV cards within 18 hours of cardholder separation. To ensure access is revoked swiftly, Federal managers, such as first-line supervisors and contracting officer's representatives, must notify system administrators when employees or contractors no longer require access to DHS information systems.[11]

We analyzed DHS data for 137,375 cardholders who separated from DHS from FY 2018 through FY 2021 and determined that DHS did not always revoke PIV cards within 18 hours as OMB recommends. According to our analysis, DHS:

- revoked 70,065 (51 percent) cards within 18 hours of cardholder separation;
- did not revoke 67,310 (49 percent) cards within 18 hours of cardholder separation, including 30,536 cards that it revoked late; and
- may not have revoked 36,774 cards (DHS officials did not record revocation dates for these cards in IDMS).

Table 1 summarizes the time it took DHS officials to revoke separated cardholders' PIV cards, according to IDMS records.

[9] *DHS National Security Systems Handbook*, Version 2.1, July 26, 2004, Sections 5.2 and 4.1.5.2.

[10] OMB M-06-06, *Sample Privacy Documents for Agency Implementation of HSPD-12*, February 17, 2006.

[11] *DHS PCI Operations Plan*, Section 8.6.

Table 1. DHS PIV Card Revocation from FY 2018 through FY 2021

Revocation Timeframe		Number of Cards	Total
Revoked within 18 Hours		70,065	70,065
Not Revoked within 18 Hours	Within 14 Days	8,188	67,310
	Within 60 Days	7,395	
	Within 180 Days	6,078	
	After 180 Days	8,875	
	May Not Have Been Revoked	36,774	

Source: DHS OIG analysis of DHS data

The revocation delays occurred because DHS did not have an adequate mechanism to ensure managers promptly notified security officials when cardholders separated from the Department. Although DHS requires managers to notify security officials that an individual has separated, managers did not always adhere to that guidance. In addition, DHS' guidance does not clearly specify when the notification must take place. Specifically, the *DHS PCI Operations Plan* requires that PIV cards be revoked within 18 hours after security officials receive notification of separation. However, the plan does not specify a timeframe for managers to notify security officials after a cardholder separates. To compensate for late or absent notifications, some security officials used an ad hoc process of comparing a 2-week-old National Finance Center report to IDMS to determine if employees had separated.

Further, DHS did not have a mechanism to ensure security officials recorded PIV card revocation dates in IDMS as the *DHS PCI Operations Plan* requires. Instead, IDMS allowed users to bypass the revocation date field without entering a date. Some DHS officials also told us they intentionally did not enter a revocation date after revoking PIV cards because doing so caused reports to become too large, resulting in IDMS slowing down.[12] For records missing revocation dates in IDMS, it was impossible for DHS OIG to conclusively determine if DHS officials revoked PIV card access promptly or at all.

We reported on similar findings in a prior audit[13] of the Department's controls to restrict access to its systems and data. Specifically, we reported that U.S. Citizenship and Immigration Services (USCIS) did not consistently manage or remove access for its personnel once they departed positions within the component.

[12] DHS management said that this problem has been resolved.

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

Although DHS officials acknowledged that thousands of PIV cards that should have been revoked were not, they calculated 22,878 PIV cards as opposed to the 36,774 we identified. According to DHS officials, they were not required to revoke the remaining 13,896 PIV cards because:

- DHS officials revoked the cards before the dates included in our analysis;
- the employees transferred within the same component; or
- the certificates or the cards had expired.

Additionally, DHS officials said they did not always enforce existing revocation policy and revoke all PIV cards whether they were collected or not. DHS officials assured us that although some PIV cards were not revoked, all tokens[14] were revoked, preventing access to electronic systems.

DHS Did Not Always Destroy PIV Cards

DHS policy requires that PIV cards be destroyed no later than 90 days after they are returned to the issuing office and revoked.[15] Security officials must also update IDMS to reflect the destruction.[16]

We analyzed the 137,375 separated cardholders' records and determined DHS did not always destroy PIV cards within 90 days. Of the 137,375 records we analyzed, DHS:

- destroyed 77,677 (56 percent) cards within 90 days of revocation;
- did not destroy 59,698 (44 percent) cards within 90 days of revocation, including 3,622 cards it destroyed late; and
- may not have destroyed 56,076 cards (DHS officials did not enter destruction dates for these cards in IDMS).

Table 2 summarizes the time it took DHS officials to destroy separated cardholders' PIV cards, according to IDMS records.

[14] A token is like an electronic key imbedded in the PIV card's chip. It is used to prove an individual's identity in conjunction with entering the correct personal identification number.
[15] *DHS PCI Operations Plan*, Section 8.6.2 (referencing DHS/All--026 Personal Identity Verification Management System Systems of Records, 74 Fed. Reg. 30,301 (June 25, 2009)).
[16] *DHS PCI Operations Plan*, Section 4.4.2.1.

Table 2. DHS PIV Card Destruction from FY 2018 through FY 2021

Destruction Timeframe		Number of Cards	Total
Destroyed within 90 Days		77,677	77,677
Not Destroyed within 90 Days	Within 180 Days	1,316	59,698
	After 180 Days	2,306	
	May Not Have Been Destroyed	56,076	

Source: DHS OIG analysis of DHS data

DHS officials acknowledged that thousands of PIV cards were not destroyed, but they calculated 39,772 PIV cards rather than the 56,076 that we reported. DHS could not explain why it destroyed PIV cards late or not at all. Without a recorded destruction date, it is difficult to conclusively establish how many PIV cards DHS officials destroyed within 90 days as required. Further, we could not determine the severity of the security risks raised by the PIV cards that remain unaccounted for.

DHS Did Not Always Withdraw Separated Individuals' Security Clearances

When a cleared individual separates from a DHS position, DHS officials must withdraw the assigned security clearance, update ISMS to reflect the separation, and terminate DHS' interest in the individual's clearance.[17] Although DHS requires DHS officials to withdraw a security clearance as soon as an individual separates from a position, DHS does not give a specific timeframe (e.g., number of hours) to do so. For our analysis, we used 1 day as the baseline.

We analyzed security records from ISMS for 98,234 cleared individuals who separated from DHS from FY 2018 through FY 2021 and determined DHS did not always withdraw separated individuals' security clearances as required. According to our analysis, DHS:

- withdrew 44,580 (45 percent) security clearances within 1 day;
- did not withdraw 80 (less than 1 percent) security clearances within 1 day, which included 11 security clearances it withdrew late and 69 clearances it did not withdraw; and
- may not have withdrawn security clearances for 53,574 (54 percent) individuals.

[17] DHS Instruction 121-01-007-01, *The Department of Homeland Security Personnel Security, Suitability and Fitness Program*, Revision 01, issued August 8, 2016, and updated June 14, 2017 (referencing ISMS quick reference guides), and ISMS Quick Guide - *Separation Process*, March 20, 2014.

Of the 69 separated individuals whose security clearances DHS did not withdraw, 5 also had PIV cards that DHS neither revoked nor destroyed. Of the 53,574 individuals whose security clearance status remained unknown, 1,272 also had PIV cards that DHS did not revoke or destroy.

Table 3 summarizes the time it took DHS officials to withdraw separated individuals' security clearances, according to ISMS.

Table 3. DHS Security Clearance Withdrawal from FY 2018 through FY 2021

Clearance Withdrawal Timeframe		Number of Individuals	Total
Withdrawn within 1 Day		44,580	44,580
Not Withdrawn within 1 Day	Within 14 Days	6	80
	Within 60 Days	1	
	Within 180 Days	2	
	After 180 Days	2	
	Clearance Not Withdrawn	69	
Unknown Status		53,574	53,574

Source: DHS OIG analysis of ISMS data

DHS security officials did not always update ISMS records for security clearance levels, statuses, and withdrawals, making it impossible to determine if DHS withdrew security clearances for the 53,574 individuals whose clearance status remains unknown. DHS officials could not tell us why they did not withdraw some security clearances or input security clearance withdrawal dates in ISMS as required when individuals separated. However, DHS officials explained that some late withdrawals had occurred because managers did not promptly notify security officials when individuals separated from the Department. According to DHS officials, it would be possible for DHS to implement a mechanism to automatically withdraw security clearances in ISMS and revoke PIV cards in IDMS based on separation. However, DHS would have to implement other policies and processes to handle PIV card revocations for other reasons.

Overall, the issues we found with revoking and destroying PIV cards and withdrawing security clearances occurred because DHS did not effectively manage and monitor IDMS and ISMS or ensure DHS officials followed offboarding processes. Without effective PIV card and security clearance management and monitoring, DHS cannot ensure only authorized individuals have access to its controlled systems and facilities. As a result, there is a risk that individuals who no longer require access to systems and facilities could circumvent controls and enter DHS buildings and controlled areas.

Recommendations

Recommendation 1: We recommend that the DHS Chief Security Officer clarify policies and procedures to require managers to notify security officials to revoke personal identity verification cards and withdraw security clearances within a specific timeframe after individuals separate from DHS.

Recommendation 2: We recommend that the DHS Chief Security Officer strengthen internal processes to ensure accountability and oversight for all personal identity verification cards that are collected and destroyed when individuals separate from DHS.

Recommendation 3: We recommend that the DHS Chief Security Officer implement additional controls to ensure personal identity verification card revocation and card destruction are completed and recorded when individuals separate from DHS.

Recommendation 4: We recommend that the DHS Chief Security Officer implement controls to ensure DHS officials record security clearance withdrawal dates in the Integrated Security Management System when individuals separate from DHS.

Recommendation 5: We recommend that the DHS Chief Security Officer develop and implement a solution to verify and validate the personal identity verification card access termination process across the Department and a mechanism to monitor its effectiveness.

Recommendation 6: We recommend that the DHS Chief Security Officer develop and implement a solution to verify and validate the security clearance withdrawal process across DHS and a mechanism to monitor its effectiveness.

Management Comments and OIG Analysis

DHS' Director, Departmental Audit Liaison provided written comments in response to our draft of this report. Appendix B contains DHS' management response in its entirety. In its management response, DHS concurred with all six report recommendations. We consider all six recommendations open and resolved. Although DHS concurred with all recommendations, its management response highlighted several concerns regarding the underlying audit work.

First, DHS asserted that our report contains inaccuracies and lacks context for metrics in the findings. Specifically, DHS expressed concern about the personnel separations, clearance withdrawals, and PIV card revocation and destruction numbers we used. We noted in the report the limitations of our data analysis and acknowledged that we could not determine the exact magnitude of the issue because records in DHS' information systems were incomplete. We also acknowledged the difference in the results of OIG's and DHS' analyses in the report and listed possible reasons for the differences according to DHS officials. Although we did not agree on the exact number of PIV cards DHS did not revoke or destroy, both DHS and OIG agreed it was tens of thousands.

Second, according to DHS, its inability to reconcile the numbers in our findings will adversely affect DHS' ability to address our recommendations. We disagree with this assertion because reconciling the number of PIV cards revoked or destroyed is not necessary for DHS to implement mechanisms and strengthen policies, procedures, and oversight to improve the Department's controls over separated individuals' PIV card access and security clearances.

Finally, DHS asserted that security clearances are not terminated or withdrawn and do not expire just by virtue of an individual leaving an organization for routine separation or offboarding. Although we agree security clearances are not terminated or expire just because an employee separates from an organization, DHS officials must withdraw the assigned security clearance eligibility and update ISMS when a cleared individual separates from a DHS position. Further, although DHS noted that in our audit, we did not review any data related to administration of Form SF-312, *Classified Information Nondisclosure Agreement,* we performed procedures to ensure the data we used was sufficiently reliable for the purposes of our audit.

DHS Response to Recommendation 1: Concur. DHS OCSO is currently pursuing a solution to streamline and automate new and existing PIV card revocation and destruction processes in IDMS and ISMS. DHS plans to fully implement these enhancements by February 2024. In the interim, OCSO, the

DHS HSPD-12 Program, and the National Security Services Division Personnel Security Program Management Office will review and clarify current policies, including responsibilities and procedures to revoke PIV card access and withdraw security clearances within a specified timeframe for separated individuals, by June 2023. OCSO will submit any policy revisions to the Department for review by September 2023 and will issue updated policies by December 2024. OCSO will communicate immediate guidance to the Department through provisional directives, including guidance to enforce the 18-hour PIV card revocation policy.

OIG Analysis: We consider these actions responsive to the recommendation, which we consider open and resolved. We will close this recommendation when DHS submits documentation showing that it has clarified and reiterated existing policies and procedures and implemented additional controls to ensure PIV card revocation and destruction are completed and recorded when individuals separate from DHS.

DHS Response to Recommendation 2: Concur. OSCO is working with the DHS Office of the Chief Readiness Support Officer to develop policy revisions that strengthen accountability and oversight. On October 13, 2022, the Office of the Chief Readiness Support Officer published DHS Personal Property Bulletin 2023-001, *Personal Identity Verification (PIV) Cards Sensitivity Elevation*, as a department-wide notification to inform personnel that DHS increased the sensitivity designation of PIV cards from Equipment Control Class Level 3 to Equipment Control Class Level 1. In addition, OCSO is updating existing policies and procedures to include remedial actions for personnel who do not destroy PIV cards or document destruction promptly. DHS plans to implement these controls by February 2024.

Further, OCSO plans to assess PIV card collection, revocation, and destruction processes at its DHS credentialing facilities annually for compliance with NIST Special Publication 800-79-2. The assessments will include document review, interviews, process testing, and observations.

Further, the DHS HSPD-12 Program, in collaboration with the DHS Office of the Chief Information Officer (OCIO), is:

- developing new automated workflows for data sharing between DHS access, credential, identity, and security management systems by March 2023;
- finalizing data sharing models and the associated interface control document and interconnection security agreement by June 2023;
- deploying new system interfaces by September 2023; and

- planning to begin onboarding DHS components to the enhanced automated solution by December 2023.

OIG Analysis: We consider these actions responsive to the recommendation, which we consider open and resolved. We will close this recommendation when DHS submits documentation showing its updated policies, procedures, and security agreement strengthening internal processes to ensure accountability and oversight for all PIV cards that are collected and destroyed when individuals separate from DHS.

DHS Response to Recommendation 3: Concur. OCSO will update existing policies and procedures to include remedial actions for personnel who do not destroy and document PIV card destruction promptly. Also, OCSO is implementing technological mechanisms to mitigate human errors. OCSO plans to use a new Technology Refresh Project to modernize DHS' infrastructure and, among other things, better track and enforce PIV card revocation and destruction. DHS plans to implement these enhancements by February 2024. In addition, OCSO will assess PIV card collection, revocation, and destruction processes at DHS credentialing facilities annually for compliance with NIST Special Publication 800-79-2.

Further, the DHS HSPD-12 Program, in collaboration with OCIO, plans to develop and deploy new data-sharing workflows and interfaces, as summarized above in the DHS response to Recommendation 2.

In addition, OCSO is augmenting the existing PIV lifecycle management process with new technology. Specifically, DHS is implementing a physical access control system (PACS), which will support PIV card revocation compliance and reduce threats associated with potential unauthorized entry using a lost, expired, or stolen PIV card by automatically de-activating the card in all connected Federal Identity Credential Access Management PACS in near real-time when a certificate is revoked or expires. DHS plans to complete these actions by February 2024.

OIG Analysis: We consider these actions responsive to the recommendation, which we consider open and resolved. We will close this recommendation when DHS provides documentation showing that the planned corrective actions are completed.

DHS Response to Recommendation 4: Concur. DHS is pursuing enhancements to its existing Identity, Credential, and Access Management architecture to implement near real-time data sharing through the Trusted Identity Exchange and ALM systems to ensure that security clearance withdrawal dates are promptly recorded in ISMS when individuals separate from DHS. DHS plans to fully implement these enhancements by February 2024.

In the interim, the DHS HSPD-12 Program, in collaboration with OCIO, plans to develop and deploy new data-sharing workflows and interfaces, as summarized above in the DHS response to recommendation 2.

OIG Analysis: We consider these actions responsive to the recommendation, which we consider open and resolved. We will close this recommendation when DHS provides documentation showing that the planned corrective actions are completed.

DHS Response to Recommendation 5: Concur. DHS is pursuing technological improvements to verify and validate the PIV card access termination process across the Department, as well as a mechanism to monitor effectiveness, which it plans to fully implement by February 2024.

In the interim, the DHS HSPD-12 Program is implementing the DHS PACS Connector, which will automate the process of revoking facility access privileges across the Department when a PIV card is deactivated in IDMS. DHS plans to finalize the governance documents for the DHS PACS Connector by December 2023. The Federal Emergency Management Agency, U.S. Immigration and Customs Enforcement, the Transportation Security Administration's HQ, and the DHS HQ's St. Elizabeth's campus are tentatively scheduled to transition to the PACS Connector during FY 2023. All other DHS components and facilities will begin the transition in FY 2024.

In addition, the DHS HSPD-12 Program, in collaboration with OCIO, plans to develop and deploy new data-sharing workflows and interfaces, as summarized above in the DHS response to Recommendation 2.

OIG Analysis: We consider these actions responsive to the recommendation, which we consider open and resolved. We will close this recommendation when DHS provides documentation showing that the planned corrective actions are completed.

DHS Response to Recommendation 6: Concur. DHS is pursuing technological improvements to automate existing processes necessary to verify and validate security clearance withdrawals in ISMS, as well as a mechanism to monitor effectiveness. DHS expects that the improvements will be available by February 2024.

In the interim, the DHS HSPD-12 Program, in collaboration with OCIO, plans to develop and deploy new data-sharing workflows and interfaces, as summarized above in the DHS response to Recommendation 2.

As an additional control, OCSO will audit and distribute monthly reports to DHS components beginning on January 3, 2023, to monitor compliance and ensure components take action to resolve all identified discrepancies in their security clearance data for inactive positions. Further, OCSO will pursue robotics process automation to enhance data analytics and discrepancy remediation.

OIG Analysis: We consider these actions responsive to the recommendation, which we consider open and resolved. We will close this recommendation when DHS provides documentation showing that the planned corrective actions are completed.

Objective, Scope, and Methodology

The Department of Homeland Security Office of Inspector General was established by the *Homeland Security Act of 2002* (Public Law 107−296) by amendment to the *Inspector General Act of 1978*.

Our objective was to determine whether DHS terminated security clearances and PIV card access for separated employees and contractors in accordance with Federal regulations and Department policies. To answer our objective, we reviewed and analyzed:

- applicable laws, regulations, executive orders, and other guidance related to security clearances and PIV card access;
- records for individuals who separated from DHS from FY 2018 through FY 2021 available in ISMS, IDMS, ALM, and component Human Resources systems;
- process workflows;
- monitoring mechanisms such as checklists, communications, and meeting minutes;
- procedures for operating and accessing the systems and equipment used to withdraw security clearances and revoke PIV cards; and
- procedures for databases and other systems used to store, track, and manage PIV card and security clearance access.

To determine the reliability of systems and controls, we reviewed prior audit results, enterprise systems' manuals, and privacy impact assessments.

We also interviewed DHS and field office personnel responsible for security clearance and access authorization and badge issuance and recovery from:

- Cybersecurity and Infrastructure Security Agency

- DHS HQ
- Federal Emergency Management Agency
- Federal Law Enforcement Training Centers
- Federal Protective Service
- Transportation Security Administration
- U.S. Citizenship and Immigration Services
- U.S. Customs and Border Protection
- U.S. Immigration and Customs Enforcement
- United States Coast Guard
- United States Secret Service

To assess whether DHS effectively managed and monitored PIV cards and access to controlled systems and facilities, we surveyed and interviewed DHS officials and tested the Department's controls over access termination using separation data from ISMS and DHS and component Human Resource offices.

We reviewed ISMS records to determine whether DHS withdrew its interests in separated employees' and contractors' security clearances as required.

To assess the reliability of ISMS, IDMS, and ALM-generated data, we:

- obtained read-only access to ISMS and IDMS;
- compared names and separation dates to data from component Human Resource systems;
- tested data to identify anomalies such as duplicate, incomplete, or missing records;
- attended virtual walkthroughs to observe the code used to generate reports;
- traced data from 310 records back to source documents to determine if information was entered correctly; and
- interviewed DHS officials who were knowledgeable about the data.

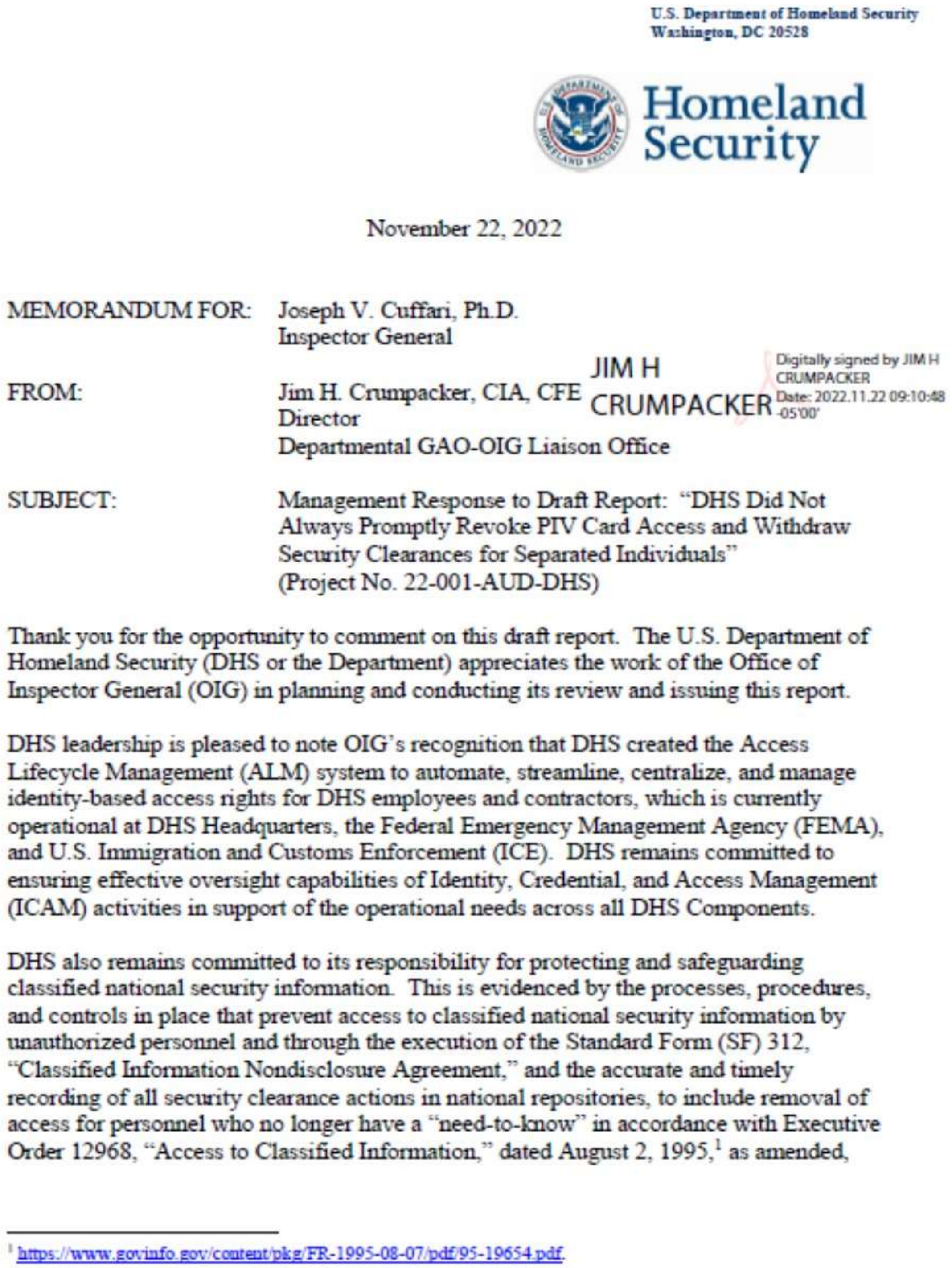
We could not match IDMS inventory information to source documents because DHS did not keep a PIV card activity log. In cases when we used computer-processed data without source documents, we performed additional procedures to ensure that the data was sufficiently reliable for the purposes of our audit; we determined that it was.

The audit also included tests of internal controls and compliance with the laws and regulations to the extent necessary to satisfy the audit objective.

We conducted this audit from October 2021 through July 2022 pursuant to the *Inspector General Act of 1978*, *as amended*, and according to the 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 objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

The Office of Audits major contributors to this report are Sean Pettersen, Director; Melissa Powe Williams, Audit Manager; Lori Smith, Auditor-in-Charge; Patricia Epperly, Auditor; Audra Morris, Auditor; Azriel Krongauz, Data Analyst; Maria Romstedt, Communications Analyst; and Nicole Kraft, Independent Referencer.

Appendix A
DHS Comments to the Draft Report



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

Homeland Security

November 22, 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: 2022.11.22 09:10:48 -05'00'

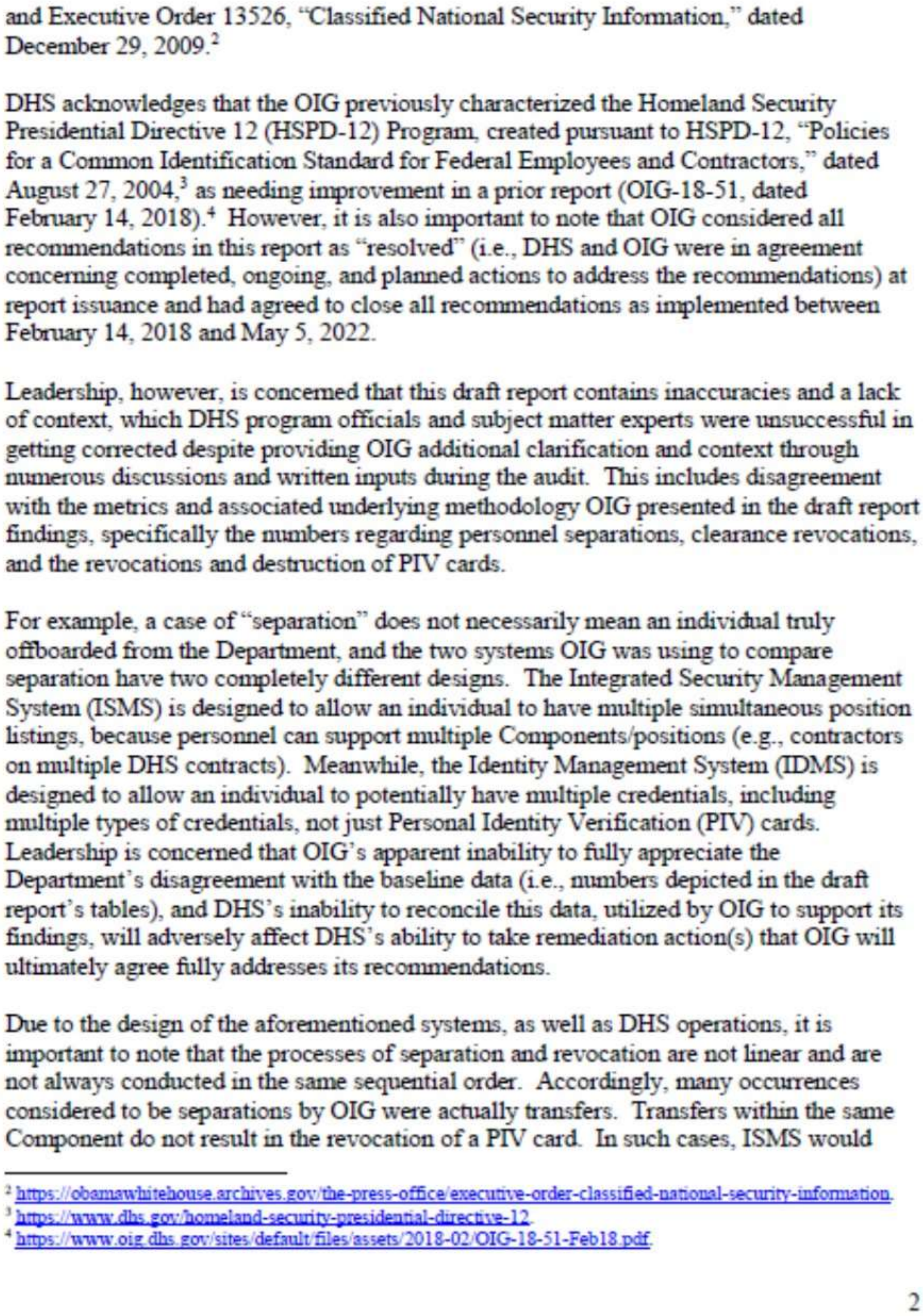
SUBJECT: Management Response to Draft Report: "DHS Did Not Always Promptly Revoke PIV Card Access and Withdraw Security Clearances for Separated Individuals"
(Project No. 22-001-AUD-DHS)

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 DHS created the Access Lifecycle Management (ALM) system to automate, streamline, centralize, and manage identity-based access rights for DHS employees and contractors, which is currently operational at DHS Headquarters, the Federal Emergency Management Agency (FEMA), and U.S. Immigration and Customs Enforcement (ICE). DHS remains committed to ensuring effective oversight capabilities of Identity, Credential, and Access Management (ICAM) activities in support of the operational needs across all DHS Components.

DHS also remains committed to its responsibility for protecting and safeguarding classified national security information. This is evidenced by the processes, procedures, and controls in place that prevent access to classified national security information by unauthorized personnel and through the execution of the Standard Form (SF) 312, "Classified Information Nondisclosure Agreement," and the accurate and timely recording of all security clearance actions in national repositories, to include removal of access for personnel who no longer have a "need-to-know" in accordance with Executive Order 12968, "Access to Classified Information," dated August 2, 1995,[1] as amended,

[1] https://www.govinfo.gov/content/pkg/FR-1995-08-07/pdf/95-19654.pdf.



and Executive Order 13526, "Classified National Security Information," dated December 29, 2009.[2]

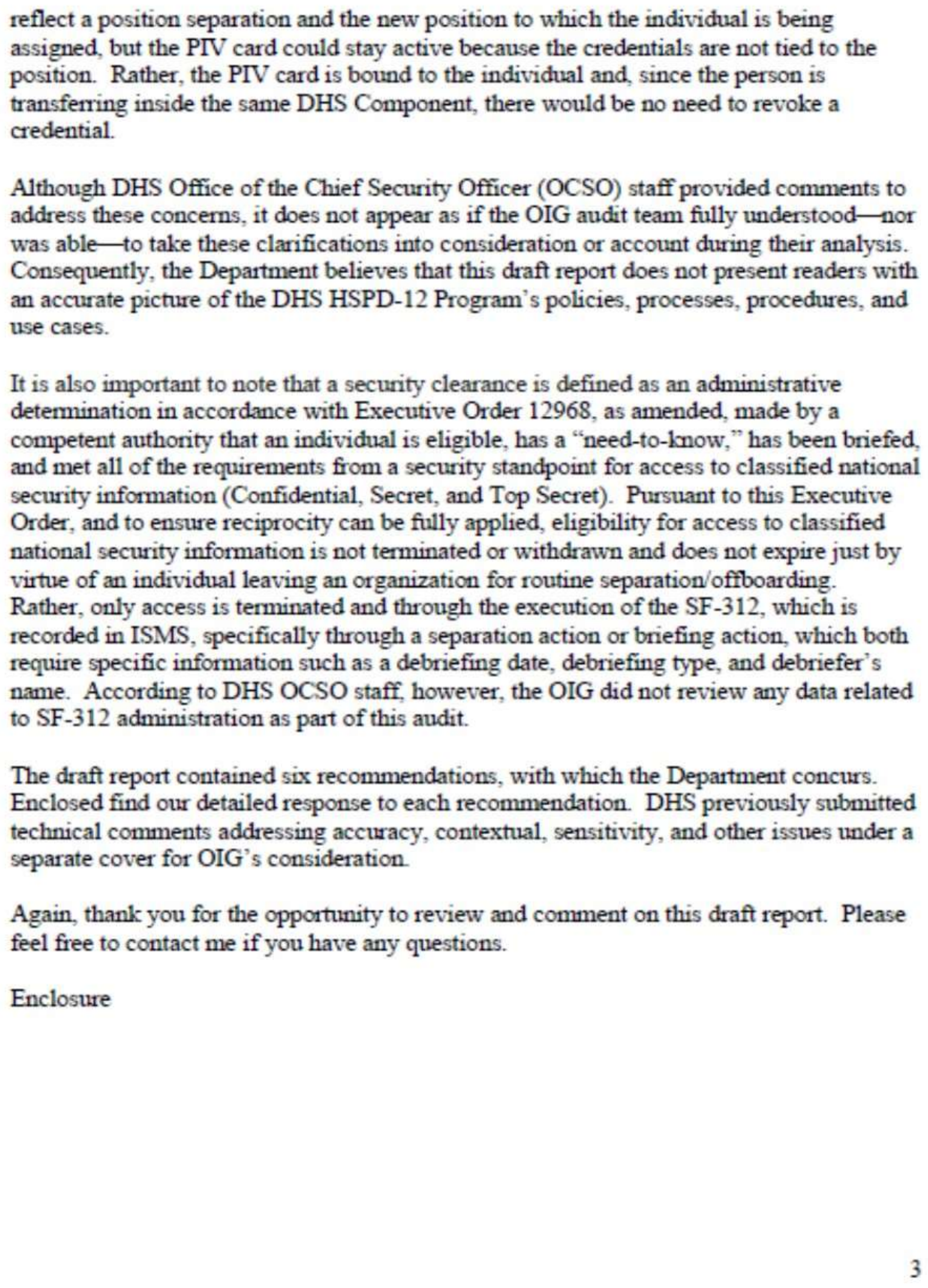
DHS acknowledges that the OIG previously characterized the Homeland Security Presidential Directive 12 (HSPD-12) Program, created pursuant to HSPD-12, "Policies for a Common Identification Standard for Federal Employees and Contractors," dated August 27, 2004,[3] as needing improvement in a prior report (OIG-18-51, dated February 14, 2018).[4] However, it is also important to note that OIG considered all recommendations in this report as "resolved" (i.e., DHS and OIG were in agreement concerning completed, ongoing, and planned actions to address the recommendations) at report issuance and had agreed to close all recommendations as implemented between February 14, 2018 and May 5, 2022.

Leadership, however, is concerned that this draft report contains inaccuracies and a lack of context, which DHS program officials and subject matter experts were unsuccessful in getting corrected despite providing OIG additional clarification and context through numerous discussions and written inputs during the audit. This includes disagreement with the metrics and associated underlying methodology OIG presented in the draft report findings, specifically the numbers regarding personnel separations, clearance revocations, and the revocations and destruction of PIV cards.

For example, a case of "separation" does not necessarily mean an individual truly offboarded from the Department, and the two systems OIG was using to compare separation have two completely different designs. The Integrated Security Management System (ISMS) is designed to allow an individual to have multiple simultaneous position listings, because personnel can support multiple Components/positions (e.g., contractors on multiple DHS contracts). Meanwhile, the Identity Management System (IDMS) is designed to allow an individual to potentially have multiple credentials, including multiple types of credentials, not just Personal Identity Verification (PIV) cards. Leadership is concerned that OIG's apparent inability to fully appreciate the Department's disagreement with the baseline data (i.e., numbers depicted in the draft report's tables), and DHS's inability to reconcile this data, utilized by OIG to support its findings, will adversely affect DHS's ability to take remediation action(s) that OIG will ultimately agree fully addresses its recommendations.

Due to the design of the aforementioned systems, as well as DHS operations, it is important to note that the processes of separation and revocation are not linear and are not always conducted in the same sequential order. Accordingly, many occurrences considered to be separations by OIG were actually transfers. Transfers within the same Component do not result in the revocation of a PIV card. In such cases, ISMS would

[2] https://obamawhitehouse.archives.gov/the-press-office/executive-order-classified-national-security-information.
[3] https://www.dhs.gov/homeland-security-presidential-directive-12.
[4] https://www.oig.dhs.gov/sites/default/files/assets/2018-02/OIG-18-51-Feb18.pdf.



reflect a position separation and the new position to which the individual is being assigned, but the PIV card could stay active because the credentials are not tied to the position. Rather, the PIV card is bound to the individual and, since the person is transferring inside the same DHS Component, there would be no need to revoke a credential.

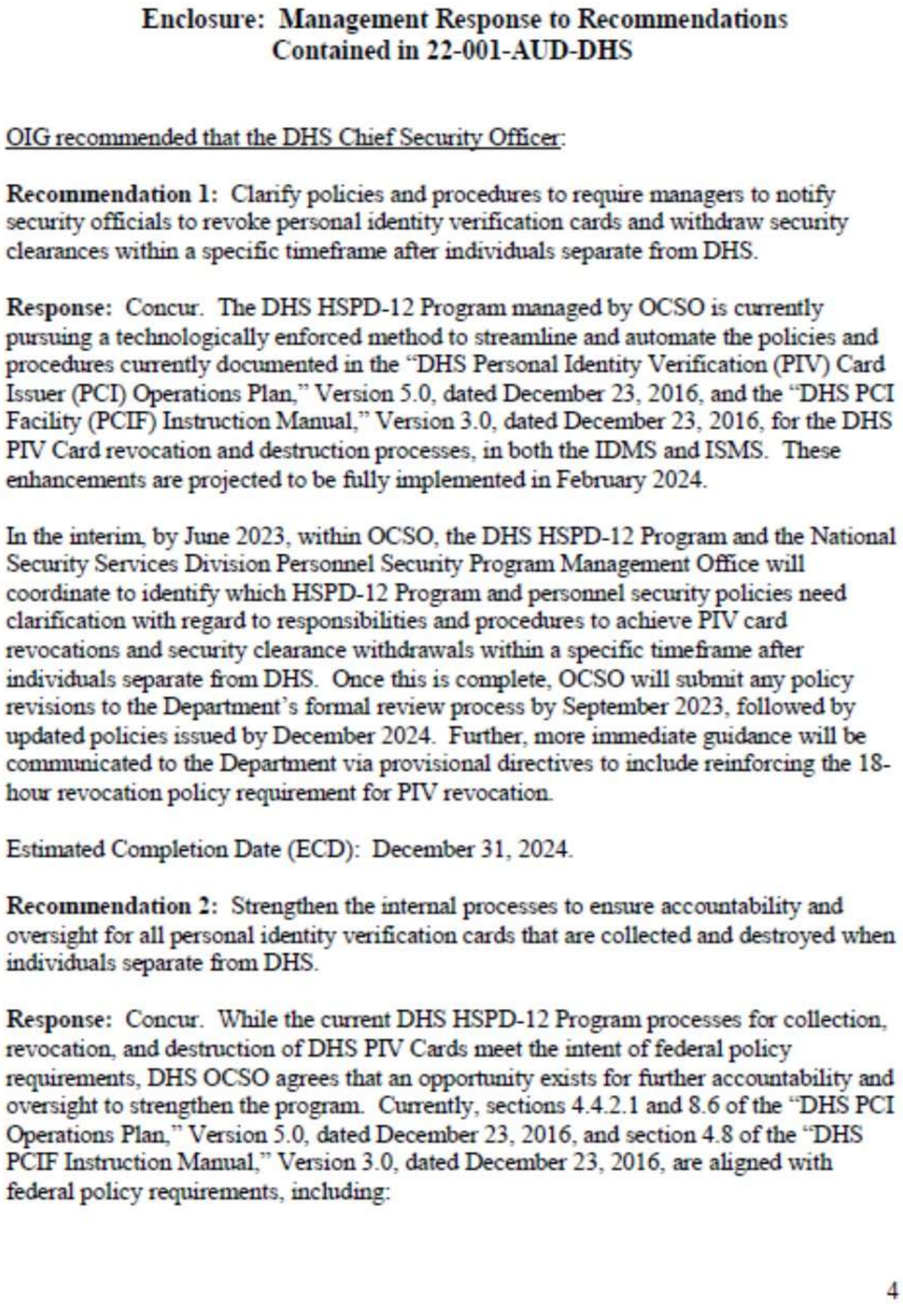
Although DHS Office of the Chief Security Officer (OCSO) staff provided comments to address these concerns, it does not appear as if the OIG audit team fully understood—nor was able—to take these clarifications into consideration or account during their analysis. Consequently, the Department believes that this draft report does not present readers with an accurate picture of the DHS HSPD-12 Program's policies, processes, procedures, and use cases.

It is also important to note that a security clearance is defined as an administrative determination in accordance with Executive Order 12968, as amended, made by a competent authority that an individual is eligible, has a "need-to-know," has been briefed, and met all of the requirements from a security standpoint for access to classified national security information (Confidential, Secret, and Top Secret). Pursuant to this Executive Order, and to ensure reciprocity can be fully applied, eligibility for access to classified national security information is not terminated or withdrawn and does not expire just by virtue of an individual leaving an organization for routine separation/offboarding. Rather, only access is terminated and through the execution of the SF-312, which is recorded in ISMS, specifically through a separation action or briefing action, which both require specific information such as a debriefing date, debriefing type, and debriefer's name. According to DHS OCSO staff, however, the OIG did not review any data related to SF-312 administration as part of this audit.

The draft report contained six recommendations, with which the Department concurs. Enclosed find our detailed response to each recommendation. DHS previously submitted technical comments addressing accuracy, contextual, sensitivity, 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.

Enclosure



Enclosure: Management Response to Recommendations Contained in 22-001-AUD-DHS

OIG recommended that the DHS Chief Security Officer:

Recommendation 1: Clarify policies and procedures to require managers to notify security officials to revoke personal identity verification cards and withdraw security clearances within a specific timeframe after individuals separate from DHS.

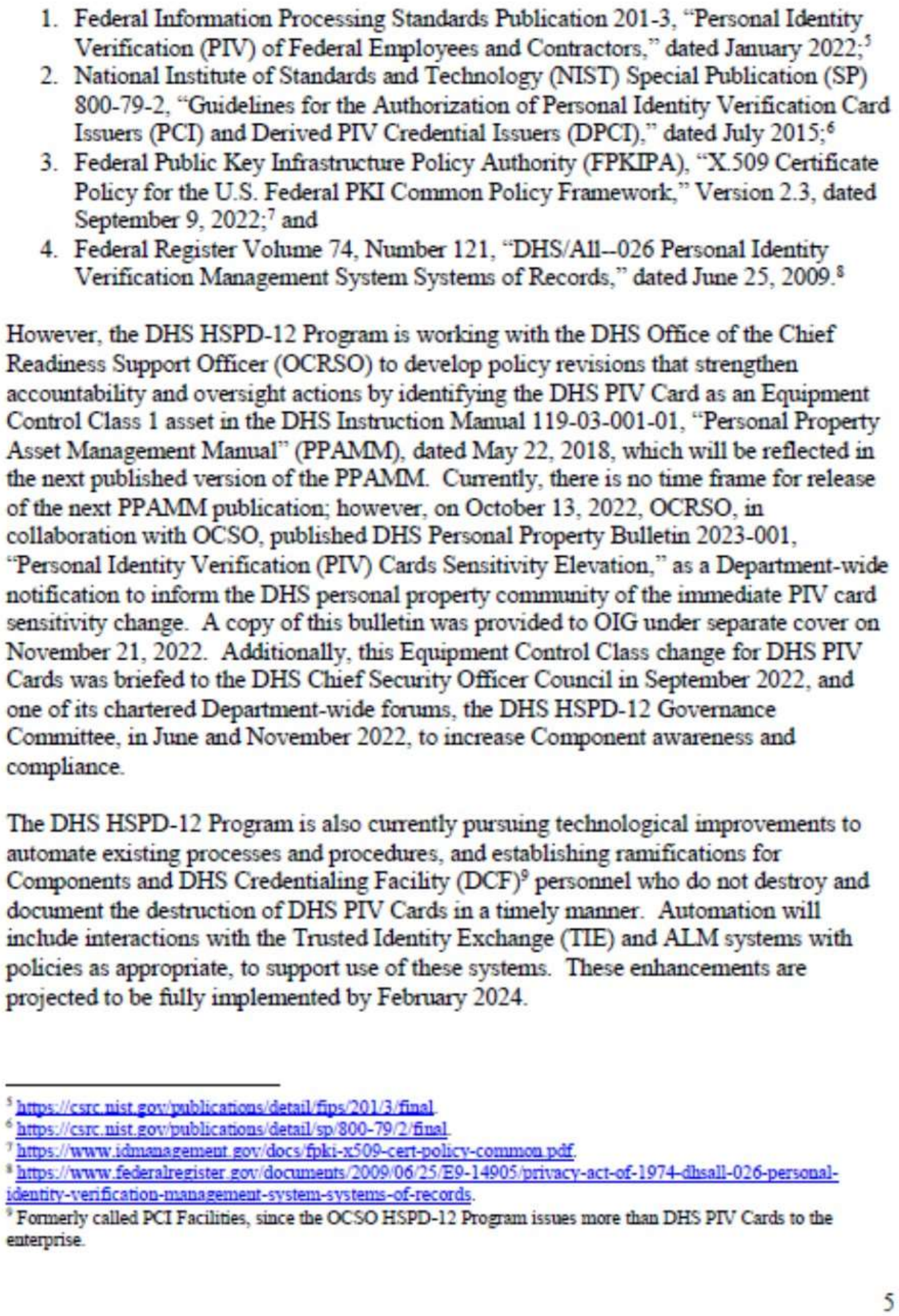
Response: Concur. The DHS HSPD-12 Program managed by OCSO is currently pursuing a technologically enforced method to streamline and automate the policies and procedures currently documented in the "DHS Personal Identity Verification (PIV) Card Issuer (PCI) Operations Plan," Version 5.0, dated December 23, 2016, and the "DHS PCI Facility (PCIF) Instruction Manual," Version 3.0, dated December 23, 2016, for the DHS PIV Card revocation and destruction processes, in both the IDMS and ISMS. These enhancements are projected to be fully implemented in February 2024.

In the interim, by June 2023, within OCSO, the DHS HSPD-12 Program and the National Security Services Division Personnel Security Program Management Office will coordinate to identify which HSPD-12 Program and personnel security policies need clarification with regard to responsibilities and procedures to achieve PIV card revocations and security clearance withdrawals within a specific timeframe after individuals separate from DHS. Once this is complete, OCSO will submit any policy revisions to the Department's formal review process by September 2023, followed by updated policies issued by December 2024. Further, more immediate guidance will be communicated to the Department via provisional directives to include reinforcing the 18-hour revocation policy requirement for PIV revocation.

Estimated Completion Date (ECD): December 31, 2024.

Recommendation 2: Strengthen the internal processes to ensure accountability and oversight for all personal identity verification cards that are collected and destroyed when individuals separate from DHS.

Response: Concur. While the current DHS HSPD-12 Program processes for collection, revocation, and destruction of DHS PIV Cards meet the intent of federal policy requirements, DHS OCSO agrees that an opportunity exists for further accountability and oversight to strengthen the program. Currently, sections 4.4.2.1 and 8.6 of the "DHS PCI Operations Plan," Version 5.0, dated December 23, 2016, and section 4.8 of the "DHS PCIF Instruction Manual," Version 3.0, dated December 23, 2016, are aligned with federal policy requirements, including:

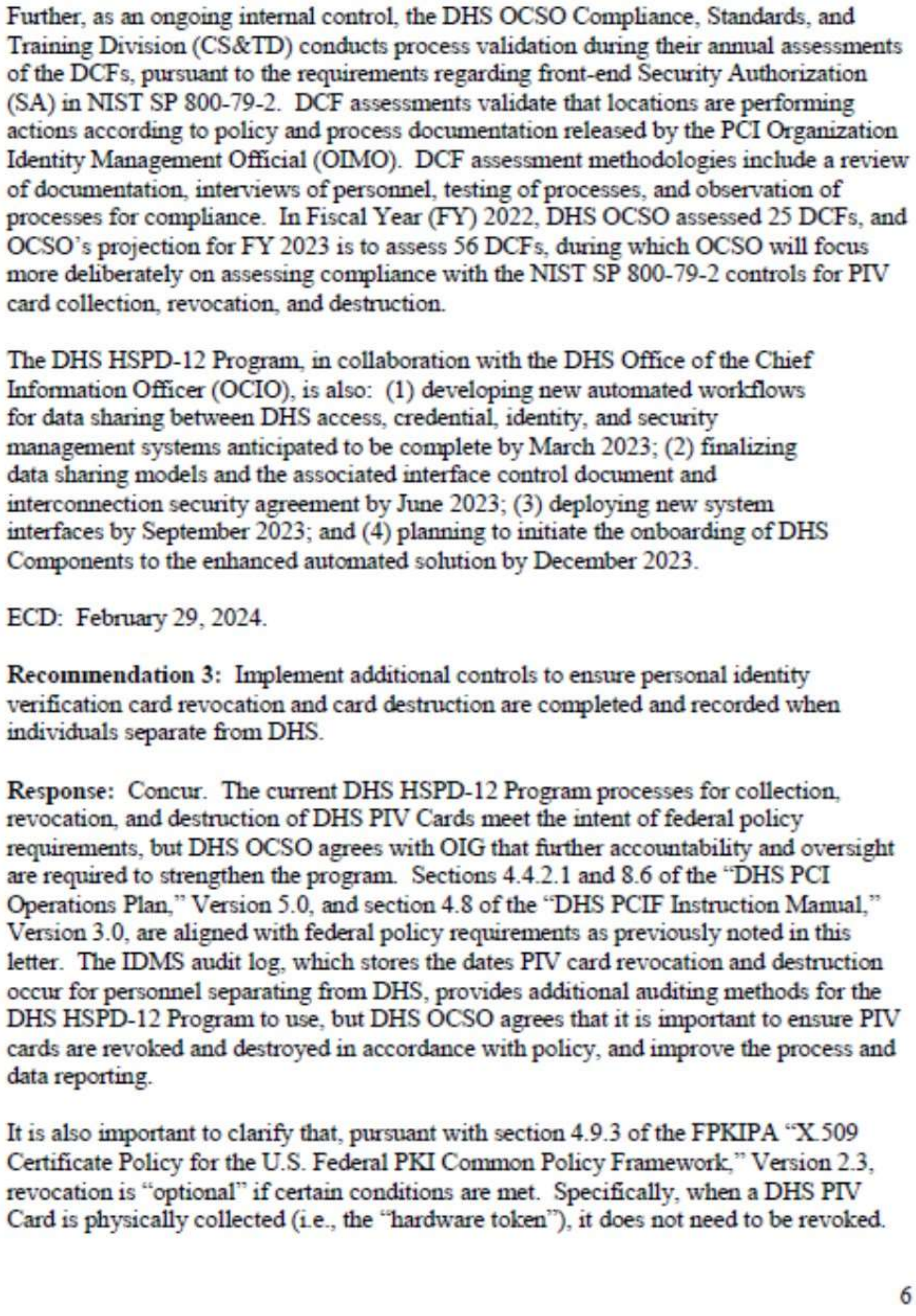


1. Federal Information Processing Standards Publication 201-3, "Personal Identity Verification (PIV) of Federal Employees and Contractors," dated January 2022;[5]
2. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-79-2, "Guidelines for the Authorization of Personal Identity Verification Card Issuers (PCI) and Derived PIV Credential Issuers (DPCI)," dated July 2015;[6]
3. Federal Public Key Infrastructure Policy Authority (FPKIPA), "X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework," Version 2.3, dated September 9, 2022;[7] and
4. Federal Register Volume 74, Number 121, "DHS/All--026 Personal Identity Verification Management System Systems of Records," dated June 25, 2009.[8]

However, the DHS HSPD-12 Program is working with the DHS Office of the Chief Readiness Support Officer (OCRSO) to develop policy revisions that strengthen accountability and oversight actions by identifying the DHS PIV Card as an Equipment Control Class 1 asset in the DHS Instruction Manual 119-03-001-01, "Personal Property Asset Management Manual" (PPAMM), dated May 22, 2018, which will be reflected in the next published version of the PPAMM. Currently, there is no time frame for release of the next PPAMM publication; however, on October 13, 2022, OCRSO, in collaboration with OCSO, published DHS Personal Property Bulletin 2023-001, "Personal Identity Verification (PIV) Cards Sensitivity Elevation," as a Department-wide notification to inform the DHS personal property community of the immediate PIV card sensitivity change. A copy of this bulletin was provided to OIG under separate cover on November 21, 2022. Additionally, this Equipment Control Class change for DHS PIV Cards was briefed to the DHS Chief Security Officer Council in September 2022, and one of its chartered Department-wide forums, the DHS HSPD-12 Governance Committee, in June and November 2022, to increase Component awareness and compliance.

The DHS HSPD-12 Program is also currently pursuing technological improvements to automate existing processes and procedures, and establishing ramifications for Components and DHS Credentialing Facility (DCF)[9] personnel who do not destroy and document the destruction of DHS PIV Cards in a timely manner. Automation will include interactions with the Trusted Identity Exchange (TIE) and ALM systems with policies as appropriate, to support use of these systems. These enhancements are projected to be fully implemented by February 2024.

[5] https://csrc.nist.gov/publications/detail/fips/201/3/final.
[6] https://csrc.nist.gov/publications/detail/sp/800-79/2/final.
[7] https://www.idmanagement.gov/docs/fpki-x509-cert-policy-common.pdf.
[8] https://www.federalregister.gov/documents/2009/06/25/E9-14905/privacy-act-of-1974-dhsall-026-personal-identity-verification-management-system-systems-of-records.
[9] Formerly called PCI Facilities, since the OCSO HSPD-12 Program issues more than DHS PIV Cards to the enterprise.



Further, as an ongoing internal control, the DHS OCSO Compliance, Standards, and Training Division (CS&TD) conducts process validation during their annual assessments of the DCFs, pursuant to the requirements regarding front-end Security Authorization (SA) in NIST SP 800-79-2. DCF assessments validate that locations are performing actions according to policy and process documentation released by the PCI Organization Identity Management Official (OIMO). DCF assessment methodologies include a review of documentation, interviews of personnel, testing of processes, and observation of processes for compliance. In Fiscal Year (FY) 2022, DHS OCSO assessed 25 DCFs, and OCSO's projection for FY 2023 is to assess 56 DCFs, during which OCSO will focus more deliberately on assessing compliance with the NIST SP 800-79-2 controls for PIV card collection, revocation, and destruction.

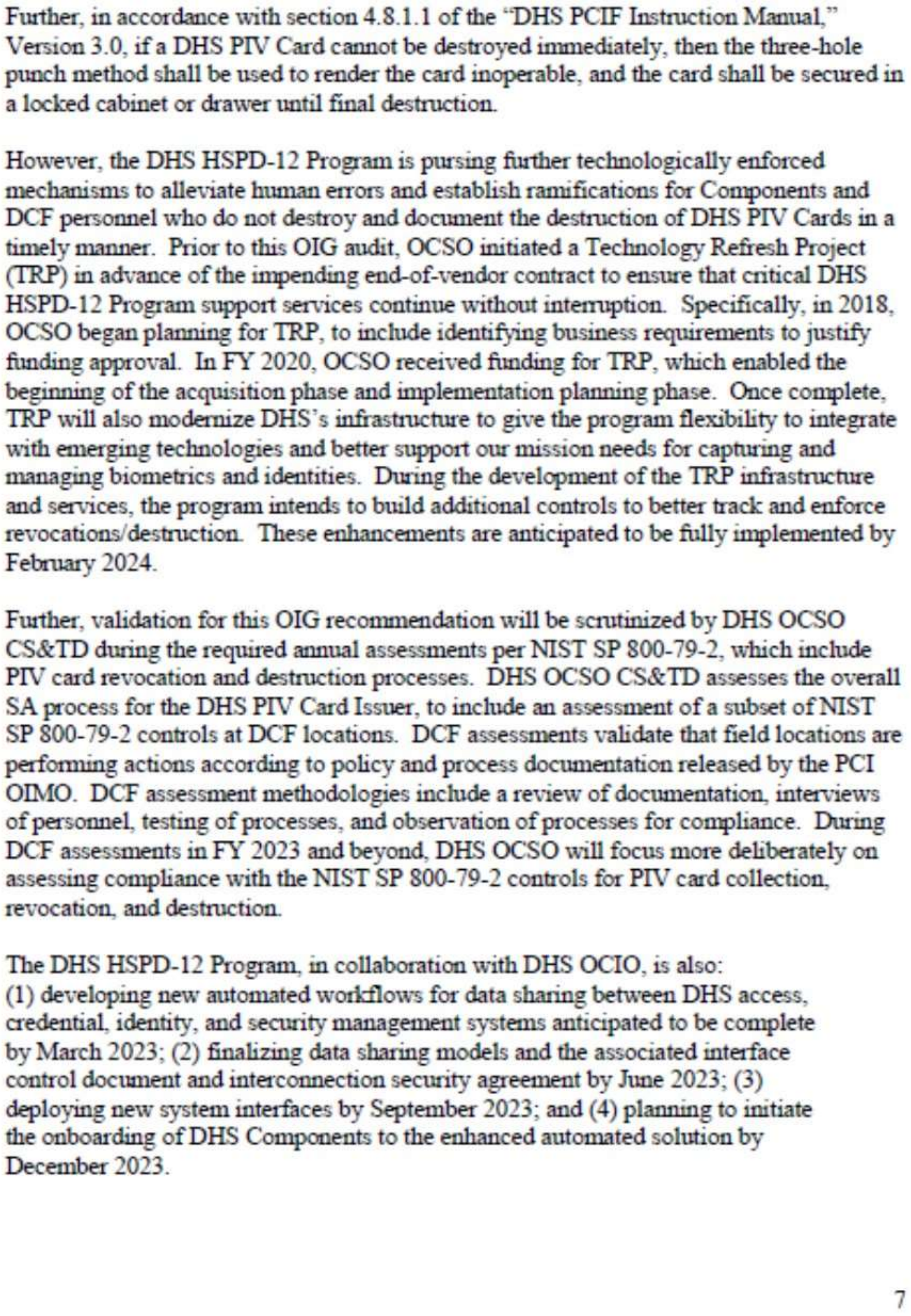
The DHS HSPD-12 Program, in collaboration with the DHS Office of the Chief Information Officer (OCIO), is also: (1) developing new automated workflows for data sharing between DHS access, credential, identity, and security management systems anticipated to be complete by March 2023; (2) finalizing data sharing models and the associated interface control document and interconnection security agreement by June 2023; (3) deploying new system interfaces by September 2023; and (4) planning to initiate the onboarding of DHS Components to the enhanced automated solution by December 2023.

ECD: February 29, 2024.

Recommendation 3: Implement additional controls to ensure personal identity verification card revocation and card destruction are completed and recorded when individuals separate from DHS.

Response: Concur. The current DHS HSPD-12 Program processes for collection, revocation, and destruction of DHS PIV Cards meet the intent of federal policy requirements, but DHS OCSO agrees with OIG that further accountability and oversight are required to strengthen the program. Sections 4.4.2.1 and 8.6 of the "DHS PCI Operations Plan," Version 5.0, and section 4.8 of the "DHS PCIF Instruction Manual," Version 3.0, are aligned with federal policy requirements as previously noted in this letter. The IDMS audit log, which stores the dates PIV card revocation and destruction occur for personnel separating from DHS, provides additional auditing methods for the DHS HSPD-12 Program to use, but DHS OCSO agrees that it is important to ensure PIV cards are revoked and destroyed in accordance with policy, and improve the process and data reporting.

It is also important to clarify that, pursuant with section 4.9.3 of the FPKIPA "X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework," Version 2.3, revocation is "optional" if certain conditions are met. Specifically, when a DHS PIV Card is physically collected (i.e., the "hardware token"), it does not need to be revoked.

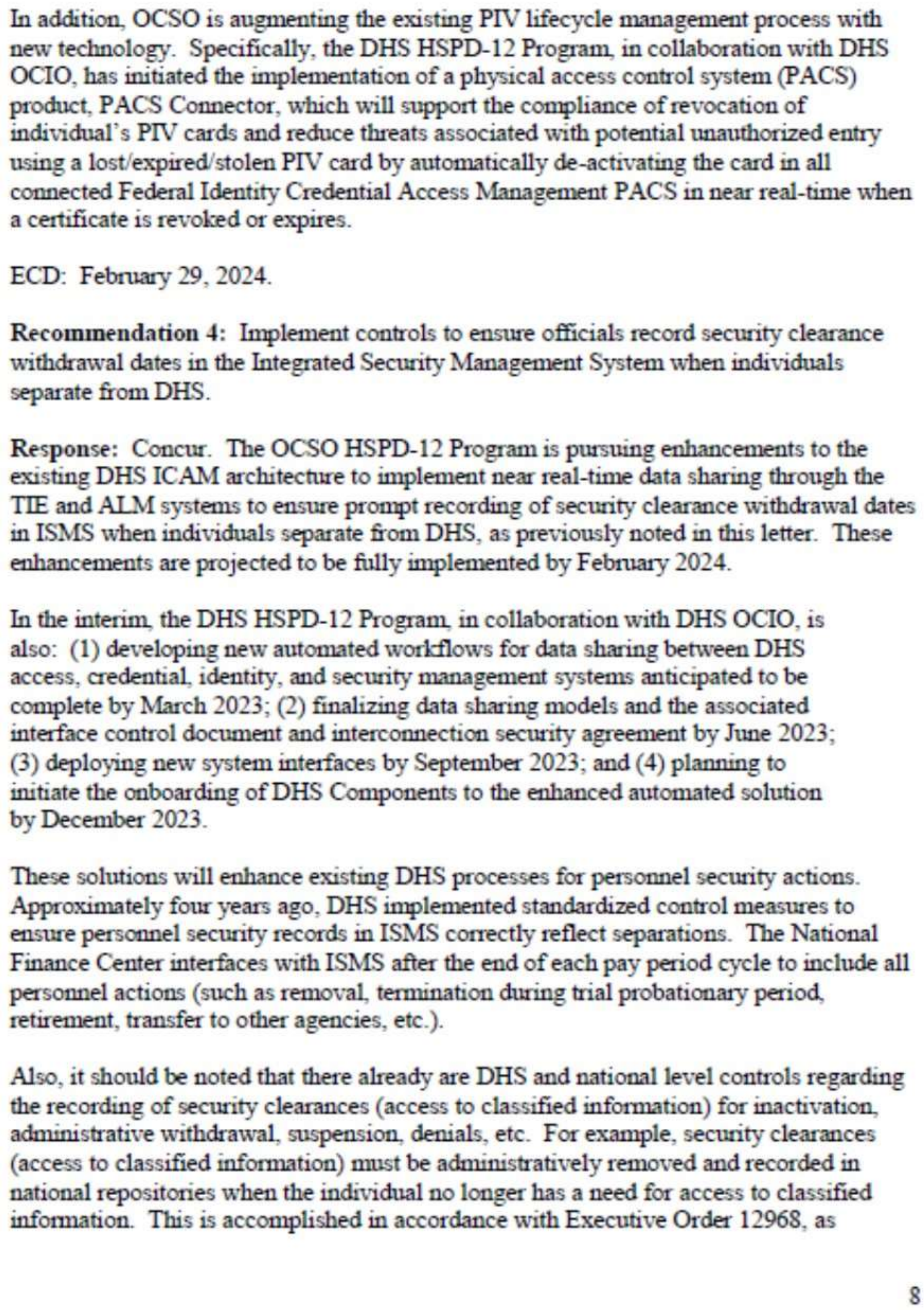


Further, in accordance with section 4.8.1.1 of the "DHS PCIF Instruction Manual," Version 3.0, if a DHS PIV Card cannot be destroyed immediately, then the three-hole punch method shall be used to render the card inoperable, and the card shall be secured in a locked cabinet or drawer until final destruction.

However, the DHS HSPD-12 Program is pursing further technologically enforced mechanisms to alleviate human errors and establish ramifications for Components and DCF personnel who do not destroy and document the destruction of DHS PIV Cards in a timely manner. Prior to this OIG audit, OCSO initiated a Technology Refresh Project (TRP) in advance of the impending end-of-vendor contract to ensure that critical DHS HSPD-12 Program support services continue without interruption. Specifically, in 2018, OCSO began planning for TRP, to include identifying business requirements to justify funding approval. In FY 2020, OCSO received funding for TRP, which enabled the beginning of the acquisition phase and implementation planning phase. Once complete, TRP will also modernize DHS's infrastructure to give the program flexibility to integrate with emerging technologies and better support our mission needs for capturing and managing biometrics and identities. During the development of the TRP infrastructure and services, the program intends to build additional controls to better track and enforce revocations/destruction. These enhancements are anticipated to be fully implemented by February 2024.

Further, validation for this OIG recommendation will be scrutinized by DHS OCSO CS&TD during the required annual assessments per NIST SP 800-79-2, which include PIV card revocation and destruction processes. DHS OCSO CS&TD assesses the overall SA process for the DHS PIV Card Issuer, to include an assessment of a subset of NIST SP 800-79-2 controls at DCF locations. DCF assessments validate that field locations are performing actions according to policy and process documentation released by the PCI OIMO. DCF assessment methodologies include a review of documentation, interviews of personnel, testing of processes, and observation of processes for compliance. During DCF assessments in FY 2023 and beyond, DHS OCSO will focus more deliberately on assessing compliance with the NIST SP 800-79-2 controls for PIV card collection, revocation, and destruction.

The DHS HSPD-12 Program, in collaboration with DHS OCIO, is also: (1) developing new automated workflows for data sharing between DHS access, credential, identity, and security management systems anticipated to be complete by March 2023; (2) finalizing data sharing models and the associated interface control document and interconnection security agreement by June 2023; (3) deploying new system interfaces by September 2023; and (4) planning to initiate the onboarding of DHS Components to the enhanced automated solution by December 2023.



In addition, OCSO is augmenting the existing PIV lifecycle management process with new technology. Specifically, the DHS HSPD-12 Program, in collaboration with DHS OCIO, has initiated the implementation of a physical access control system (PACS) product, PACS Connector, which will support the compliance of revocation of individual's PIV cards and reduce threats associated with potential unauthorized entry using a lost/expired/stolen PIV card by automatically de-activating the card in all connected Federal Identity Credential Access Management PACS in near real-time when a certificate is revoked or expires.

ECD: February 29, 2024.

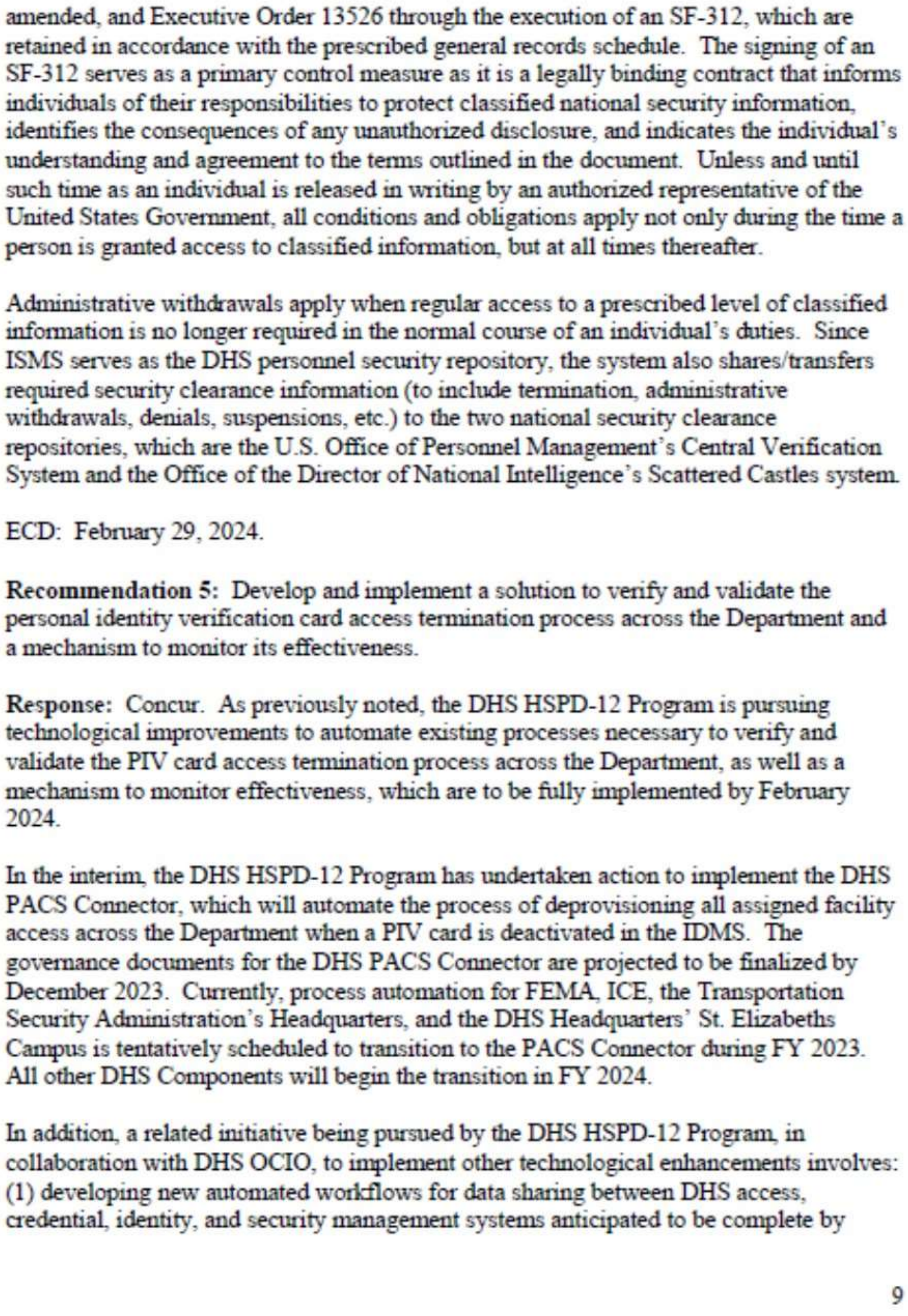
Recommendation 4: Implement controls to ensure officials record security clearance withdrawal dates in the Integrated Security Management System when individuals separate from DHS.

Response: Concur. The OCSO HSPD-12 Program is pursuing enhancements to the existing DHS ICAM architecture to implement near real-time data sharing through the TIE and ALM systems to ensure prompt recording of security clearance withdrawal dates in ISMS when individuals separate from DHS, as previously noted in this letter. These enhancements are projected to be fully implemented by February 2024.

In the interim, the DHS HSPD-12 Program, in collaboration with DHS OCIO, is also: (1) developing new automated workflows for data sharing between DHS access, credential, identity, and security management systems anticipated to be complete by March 2023; (2) finalizing data sharing models and the associated interface control document and interconnection security agreement by June 2023; (3) deploying new system interfaces by September 2023; and (4) planning to initiate the onboarding of DHS Components to the enhanced automated solution by December 2023.

These solutions will enhance existing DHS processes for personnel security actions. Approximately four years ago, DHS implemented standardized control measures to ensure personnel security records in ISMS correctly reflect separations. The National Finance Center interfaces with ISMS after the end of each pay period cycle to include all personnel actions (such as removal, termination during trial probationary period, retirement, transfer to other agencies, etc.).

Also, it should be noted that there already are DHS and national level controls regarding the recording of security clearances (access to classified information) for inactivation, administrative withdrawal, suspension, denials, etc. For example, security clearances (access to classified information) must be administratively removed and recorded in national repositories when the individual no longer has a need for access to classified information. This is accomplished in accordance with Executive Order 12968, as



amended, and Executive Order 13526 through the execution of an SF-312, which are retained in accordance with the prescribed general records schedule. The signing of an SF-312 serves as a primary control measure as it is a legally binding contract that informs individuals of their responsibilities to protect classified national security information, identifies the consequences of any unauthorized disclosure, and indicates the individual's understanding and agreement to the terms outlined in the document. Unless and until such time as an individual is released in writing by an authorized representative of the United States Government, all conditions and obligations apply not only during the time a person is granted access to classified information, but at all times thereafter.

Administrative withdrawals apply when regular access to a prescribed level of classified information is no longer required in the normal course of an individual's duties. Since ISMS serves as the DHS personnel security repository, the system also shares/transfers required security clearance information (to include termination, administrative withdrawals, denials, suspensions, etc.) to the two national security clearance repositories, which are the U.S. Office of Personnel Management's Central Verification System and the Office of the Director of National Intelligence's Scattered Castles system.

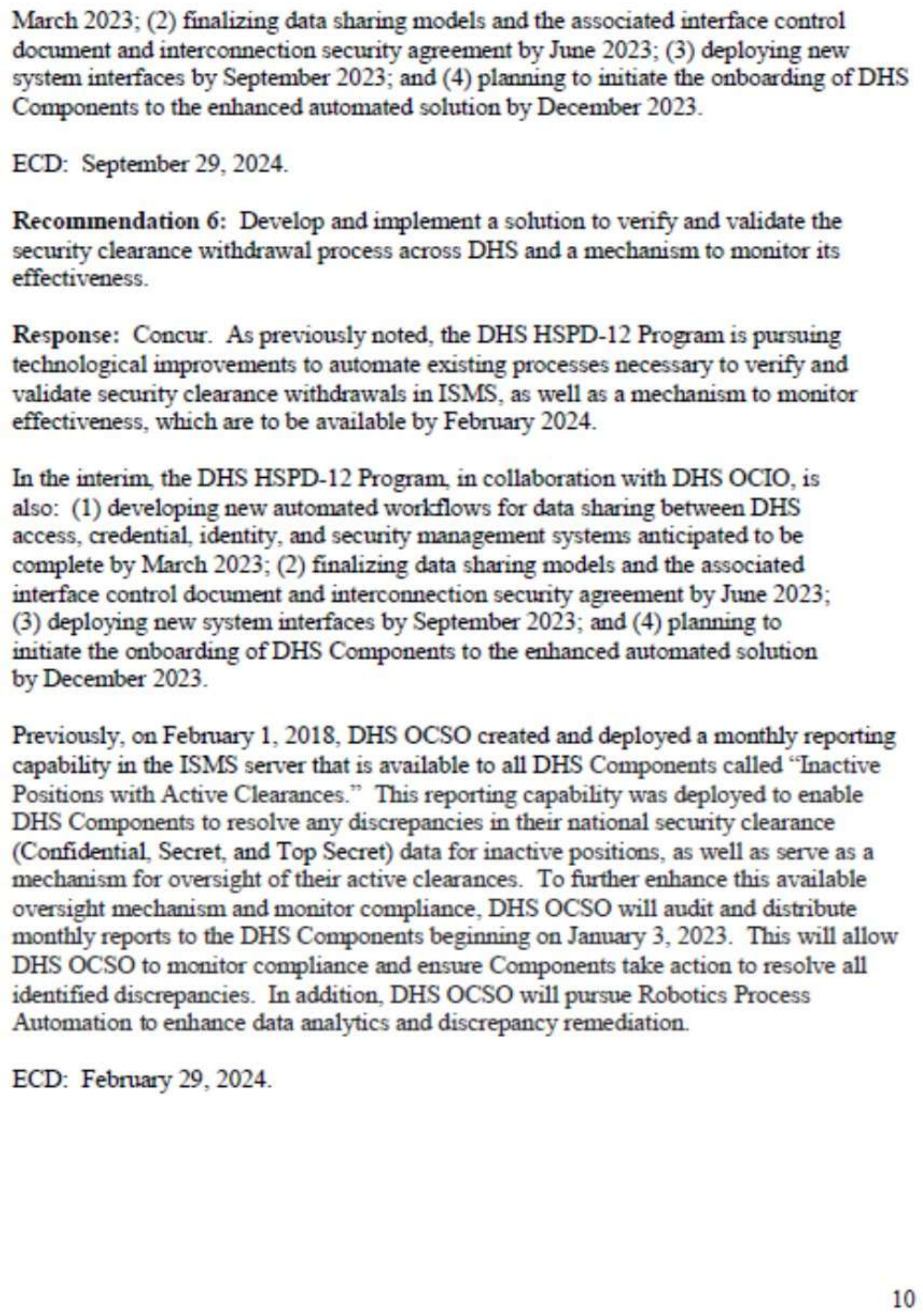
ECD: February 29, 2024.

Recommendation 5: Develop and implement a solution to verify and validate the personal identity verification card access termination process across the Department and a mechanism to monitor its effectiveness.

Response: Concur. As previously noted, the DHS HSPD-12 Program is pursuing technological improvements to automate existing processes necessary to verify and validate the PIV card access termination process across the Department, as well as a mechanism to monitor effectiveness, which are to be fully implemented by February 2024.

In the interim, the DHS HSPD-12 Program has undertaken action to implement the DHS PACS Connector, which will automate the process of deprovisioning all assigned facility access across the Department when a PIV card is deactivated in the IDMS. The governance documents for the DHS PACS Connector are projected to be finalized by December 2023. Currently, process automation for FEMA, ICE, the Transportation Security Administration's Headquarters, and the DHS Headquarters' St. Elizabeths Campus is tentatively scheduled to transition to the PACS Connector during FY 2023. All other DHS Components will begin the transition in FY 2024.

In addition, a related initiative being pursued by the DHS HSPD-12 Program, in collaboration with DHS OCIO, to implement other technological enhancements involves: (1) developing new automated workflows for data sharing between DHS access, credential, identity, and security management systems anticipated to be complete by



March 2023; (2) finalizing data sharing models and the associated interface control document and interconnection security agreement by June 2023; (3) deploying new system interfaces by September 2023; and (4) planning to initiate the onboarding of DHS Components to the enhanced automated solution by December 2023.

ECD: September 29, 2024.

Recommendation 6: Develop and implement a solution to verify and validate the security clearance withdrawal process across DHS and a mechanism to monitor its effectiveness.

Response: Concur. As previously noted, the DHS HSPD-12 Program is pursuing technological improvements to automate existing processes necessary to verify and validate security clearance withdrawals in ISMS, as well as a mechanism to monitor effectiveness, which are to be available by February 2024.

In the interim, the DHS HSPD-12 Program, in collaboration with DHS OCIO, is also: (1) developing new automated workflows for data sharing between DHS access, credential, identity, and security management systems anticipated to be complete by March 2023; (2) finalizing data sharing models and the associated interface control document and interconnection security agreement by June 2023; (3) deploying new system interfaces by September 2023; and (4) planning to initiate the onboarding of DHS Components to the enhanced automated solution by December 2023.

Previously, on February 1, 2018, DHS OCSO created and deployed a monthly reporting capability in the ISMS server that is available to all DHS Components called "Inactive Positions with Active Clearances." This reporting capability was deployed to enable DHS Components to resolve any discrepancies in their national security clearance (Confidential, Secret, and Top Secret) data for inactive positions, as well as serve as a mechanism for oversight of their active clearances. To further enhance this available oversight mechanism and monitor compliance, DHS OCSO will audit and distribute monthly reports to the DHS Components beginning on January 3, 2023. This will allow DHS OCSO to monitor compliance and ensure Components take action to resolve all identified discrepancies. In addition, DHS OCSO will pursue Robotics Process Automation to enhance data analytics and discrepancy remediation.

ECD: February 29, 2024.

Appendix B
Report Distribution

Department of Homeland Security

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

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees

Additional Information 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