

Department-wide Management of the HSPD-12 Program Needs Improvement





DHS OIG HIGHLIGHTS

Department-wide Management of the HSPD-12 Program Needs Improvement

February 14, 2018

Why We Did This Audit

Homeland Security Presidential Directive (HSPD) 12 requires that Federal agencies implement a government-wide standard for secure, reliable identification for their employees and contractors to access facilities and systems. Our objective was to assess DHS' progress in implementing and managing the HSPD-12 program since our prior audits in 2007 and 2010.

What We Recommend

We are making seven recommendations for the DHS Chief Security Officer to improve implementation and management of the HSPD-12 program.

For Further Information:

Contact our Office of Public Affairs at (202) 254-4100, or email us at DHS-OIG.OfficePublicAffairs@oig.dhs.gov

What We Found

The Department of Homeland Security has not made much progress in implementing and managing requirements of the HSPD-12 program department-wide. Many of the same issues we previously reported in 2007 and 2010 pose challenges today. For example, DHS has an effective process for issuing personal identity verification cards, which is an improvement from the 2010 report. However, it still faces significant program and management challenges in implementing an effective HSPD-12 program, such as placing priority on ensuring termination of the cards for separated contractors who no longer require access.

Further, DHS has made limited progress implementing the controls necessary to regulate access to DHS facilities and systems. At the time of our audit, no DHS component had fully addressed key physical access control requirements, such as inventorying, assigning risk levels, and identifying existing mechanisms for securing owned and leased facilities. This occurred because of insufficient guidance, funding, staffing, and oversight to ensure compliance. Additionally, although DHS components reported 99 percent compliance in implementing logical access controls on their unclassified information systems, this information had not been independently verified by the Department.

As a result of these deficiencies, DHS cannot ensure that only authorized employees have access to its controlled facilities and systems. The potential remains for individuals who misrepresent their identities to circumvent controls, enter DHS buildings and controlled areas, and cause harm to people and assets. The potential also exists for unauthorized access to information systems, which could result in loss, theft, or misuse of sensitive information.

Management Response

The Department concurred with our recommendations.



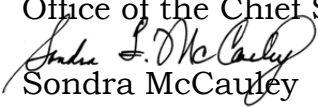
OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

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

February 14, 2018

MEMORANDUM FOR: Richard McComb
Chief Security Officer
Office of the Chief Security Office

FROM: 
Sondra McCauley
Assistant Inspector General
Office of Information Technology Audits

SUBJECT: *Department-wide Management of the HSPD-12 Program
Needs Improvement*

Attached for your action is our final report, *Department-wide Management of the HSPD-12 Program Needs Improvement*. We incorporated the formal comments provided by your office.

The report contains seven recommendations aimed at improving the implementation and management of the HSPD-12 program. Your office concurred with all of the recommendations. Based on information provided in your response to the draft report, we consider recommendations 1, 2, 3, 4, 6, and 7 open and resolved. Once your office has fully implemented the recommendations, please submit a formal closeout letter to us within 30 days so that we may close the recommendations. The memorandum should be accompanied by evidence of completion of agreed-upon corrective actions and of the disposition of any monetary amounts. Recommendation 5 is resolved and closed.

Please send your response or closure request to
OIGITAuditsFollowup@oig.dhs.gov.

Consistent with our responsibility under the *Inspector General Act*, we will provide copies of our report to congressional committees with oversight and appropriation responsibility over the Department of Homeland Security. We will post the report on our website for public dissemination.

Please call me with any questions, or your staff may contact Richard Saunders, Director, Advanced Technology Projects, at (202) 254-5440.

Attachment



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Table of Contents

Background	3
Results of Audit	11
Effective Process for PIV Card Issuance, but Additional Controls Needed for Card Termination	12
Physical and Logical Access Controls Were Not Fully Implemented in Compliance with HSPD-12 Requirements.....	17
Challenges to HSPD-12 Program Management Pose Risks to Personnel, Property, and Information.....	29
Recommendations.....	31

Appendixes

Appendix A: Objective, Scope, and Methodology	39
Appendix B: Management Comments to the Draft Report.....	41
Appendix C: Major HSPD-12 Milestones and Requirements	47
Appendix D: Detailed Description of PIV Subsystems	49
Appendix E: Office of IT Audits Major Contributors to This Report	53
Appendix F: Report Distribution.....	54

Abbreviations

ALM	Access Lifecycle Management
CBP	U.S. Customs and Border Protection
CIO	Chief Information Officer
CISO	Chief Information Security Officer
COR	Contracting Officer Representative
CSO	Chief Security Officer
ESSD	Enterprise Security Services Division
FEMA	Federal Emergency Management Agency
FIPS	Federal Information Processing Standard
FISMA	<i>Federal Information Security Modernization Act</i>
FLETC	Federal Law Enforcement Training Centers
FPS	Federal Protective Service
FSL	facility security level
HSPD-12	Homeland Security Presidential Directive 12
ICAM	Identity Credential and Access Management



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

ICC	integrated circuit chip
ICE	U.S. Immigration and Customs Enforcement
ID	identification
IDMS	Identity Management System
ISMS	Integrated Security Management System
IT	information technology
LACS	Logical Access Control System
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
OCSO	Office of the Chief Security Officer
OIG	Office of Inspector General
OMB	Office of Management and Budget
PACS	Physical Access Control System
PCI	PIV card issuer
PCIF	PIV card issuance facility
PIN	personal identification number
PIV	personal identity verification
PKI	Public Key Infrastructure
PMO	Program Management Office
TSA	Transportation Security Administration
USCIS	U.S. Citizenship and Immigration Services



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Background

Homeland Security Presidential Directive (HSPD) 12, dated August 27, 2004, established a policy for creation, issuance, and use of personal identification credentials in the Federal Government. The Directive requires the use of a standard, secure, and reliable form of identification for Federal employees and contractors. HSPD-12 required Federal agencies to begin using the standard form of identification by November 2006 to gain physical and logical access to federally controlled facilities and information systems. It also called for interoperable mechanisms for authenticating employee identity and permissions at graduated levels of security, depending on the agency environment and the sensitivity of facilities and data accessed.

The PIV Card

To support HSPD-12, the National Institute of Standards and Technology (NIST) published the 2005 Federal Information Processing Standard (FIPS) 201, which established the personal identity verification (PIV) card as a common authentication mechanism (through the use of integrated readers) across the Federal Government.¹ The PIV card is the foundation for securely identifying every individual seeking access to valuable and sensitive Federal resources, including facilities and information systems. Also known as a “Smart Card,” a PIV card is similar in size to a credit card and contains information that is either printed on the outside or stored on the card’s integrated circuit chip (ICC). Figure 1 depicts a PIV card and the information it contains.

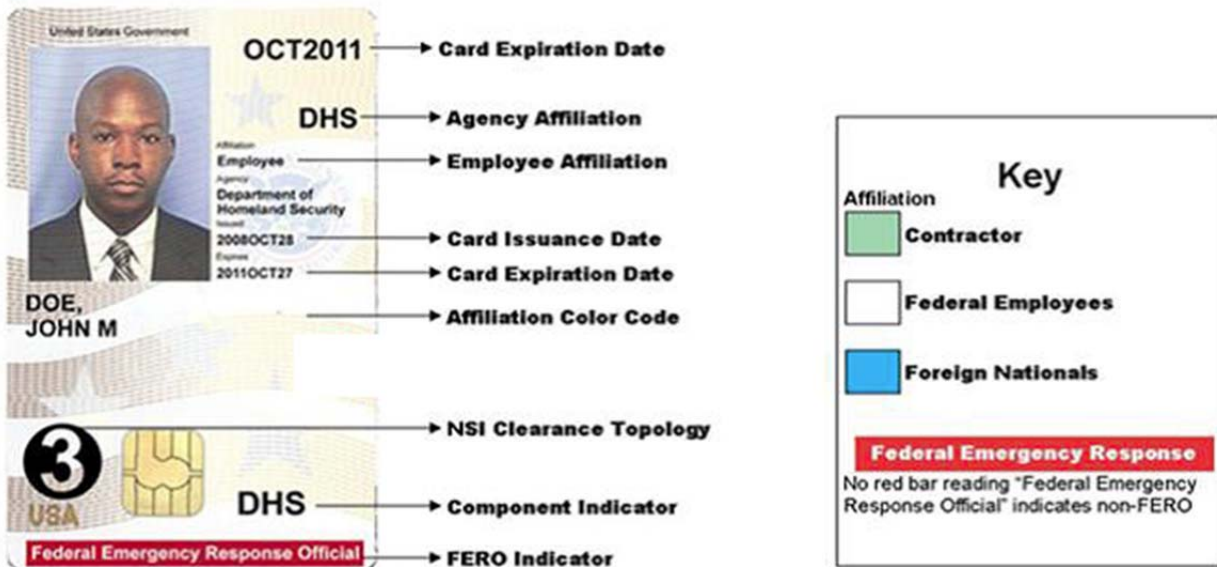
¹ FIPS 201, *Personal Identity Verification of Federal Employees and Contractors*, August 2013



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Figure 1: Key Information on a Sample PIV Card



Source: Office of Inspector General (OIG), based on an image in *DHS PCI Operations Plan, version 4*, dated February 2014

As shown, the DHS PIV card presents all elements required by FIPS. The exterior of the card includes a photograph for visual verification of the user's identity. Below the photograph is the cardholder's name. Other data elements on the PIV card include:

- Card Expiration Date: Indicating the month and year the PIV card will expire;
- Agency Affiliation: Designating the Federal agency with which the cardholder is affiliated;
- Employee Affiliation: Indicating whether the cardholder is an employee, contractor, detailee, or foreign national;
- Card Issuance Date: Indicating the day, month, and year the PIV card was issued;
- Card Expiration Date: Designating the day, month, and year the PIV card will expire;
- Affiliation Color Code: Designating the employee's affiliation by color code (as specified in the key in figure 1); and
- Component Indicator: Indicating the location of the cardholder within the agency.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

The ICC embedded on the PIV card is loaded with electronic data and software to identify the user. This includes multifactor verification of the cardholder for access to controlled facilities and systems when required.² The ICC typically includes the following data.

- card manufacturer
- card model
- credential number
- global unique identifier
- cardholder unique identifier
- cardholder biometric data, such as fingerprints
- electronic certificates for user authentication:
 - PIV authentication key
 - digital signature key

The electronic certificates are loaded onto the PIV card. When the cardholder presents the card to a physical or logical access control system, the certificate's key is processed by a card reader and physical or logical resource to help authenticate the cardholder and verify his or her access rights.³ These certificates and keys expire on predetermined dates and may be revoked by the issuer. In addition, the certificate keys are used to perform complementary operations, such as encryption and decryption of data, or signature generation and verification.

The PIV System

The PIV card is the primary component of the PIV system. It is issued to an individual to gain access to an HSPD-12 compliant physical or logical controlled asset, based on the individual's assigned privilege. Physical access refers to entry to a secured building, wing, floor, or room that a cardholder wishes to enter. In contrast, logical access is typically entry to a network or a location on a network (e.g., a computer workstation, folder, file, database record, or software program). Per FIPS 201, the PIV system is divided into three subsystems that cover PIV card lifecycle management from issuance to termination.

² NIST Special Publication 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations, Revision 4*, April 2013, defines multi-factors as: 1) something you know (e.g., password, personal identification number (PIN)); 2) something you have (e.g., PIV card); or (3) something you are (e.g., biometrics such as fingerprints).

³ Credentials on the PIV card (such as the PIV card certificates and keys) may be used in conjunction with other authentication factors (such as the successful input of a PIN or an on-card biometric comparison) to further authenticate the cardholder.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

1. Card Issuance and Management – This subsystem is responsible for identity-proofing and registration, PIV card issuance and maintenance, key management, and various repositories and services (e.g., public key infrastructure (PKI) directory or certificate status servers) required as part of the identity verification process.
2. Physical and Logical Access Points – Commonly referred to as the PIV system front-end, this subsystem consists of the PIV card, card and biometric readers, and PIN input device. The PIV cardholder interacts with the PIV system front-end to initiate physical or logical access to the desired controlled asset.
3. Cardholder Authentication and Authorization – Commonly referred to as the PIV system back-end, this subsystem facilitates the PIV cardholder identification process during attempts to access physical or logical assets. It consists of physical and logical access control systems, controlled assets, and authorization data.

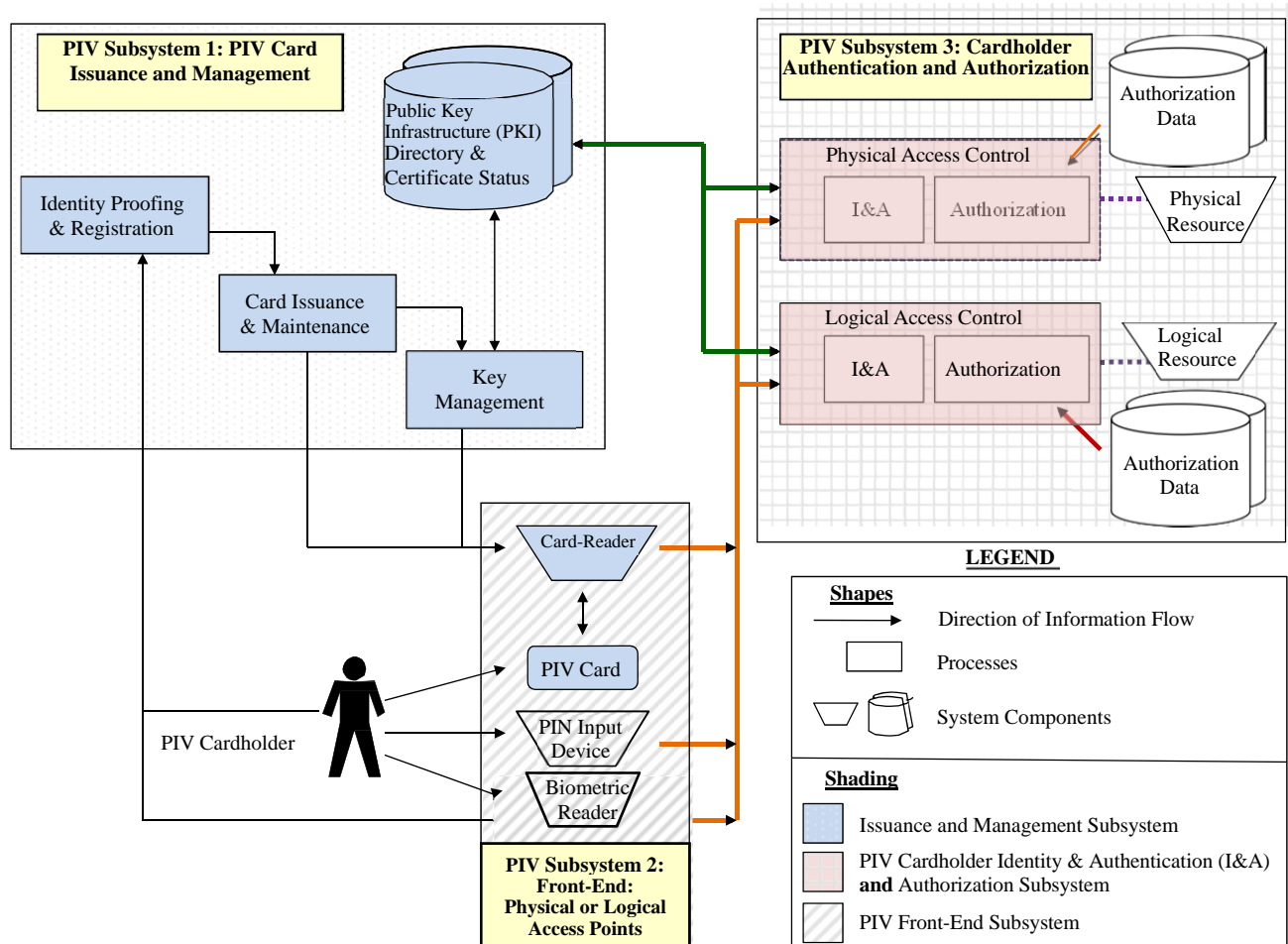
Figure 2 provides a notional view of the PIV system, including these three subsystems.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Figure 2: Notional View of the PIV System



Source: FIPS 201, *Personal Identity Verification of Federal Employees and Contractors*, August 2013

A detailed description of each of the three PIV system subsystems is located in appendix D.

Additional HSPD-12 Guidance

In 2011, to promote agency implementation of HSPD-12 requirements, the Office of Management and Budget (OMB) issued Memorandum M-11-11, directing Federal agencies to institute policy requiring the use of PIV card credentials as the primary method for authenticating users for physical and



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

logical access to Federal facilities and information systems.⁴ Policy requirements included:

- All new systems under development were to be enabled to use PIV credentials, in accordance with NIST guidelines, prior to being made operational.
- In accordance with NIST guidelines and by fiscal year 2012, existing physical and logical access control systems were to be upgraded to use PIV credentials prior to agency application of development and technology refresh funds to complete other activities.
- Procurements for services and products involving facility or system access control were to be in accordance with HSPD-12 policy and the *Federal Acquisition Regulation* rules to ensure government-wide interoperability.⁵

In 2013, OMB issued Memorandum M-14-04, *Fiscal Year 2013 Reporting Instructions for the Federal Information Security Modernization Act and Agency Privacy Management*, which identified HSPD-12 PIV card use with strong authentication as a priority across the Federal Government. Additionally, the memo emphasized OMB's expectation that all information technology (IT) system applications included as part of *Federal Information Security Modernization Act* (FISMA) reporting use PIV credentials as the means for cardholder logical access. Physical access control systems were also required to be included in the count of FISMA-reported systems.

Further, in June 2015, OMB ordered a 30-day "Cybersecurity Sprint" as a result of a massive breach of Office of Personnel Management information systems.⁶ The exercise required that all Federal agencies take immediate actions to improve the security of their information systems and data. Specified actions included strengthening access controls for authorized (and therefore trusted) system users and increasing the use of multifactor authentication, including PIV credentials.

⁴ OMB Memorandum M-11-11, *Continued Implementation of Homeland Security Presidential Directive (HSPD) 12*, dated February 2011, required agencies to use a common identification standard to gain physical access to federally-controlled facilities and logical access to federally-controlled information systems.

⁵ OMB Memorandum M-06-18, *Acquisition of Products and Services for Implementation of HSPD-12*, June 30, 2016

⁶ OMB Memorandum M-16-04, *Cybersecurity Strategy and Implementation Plan for the Federal Civilian Government*, October 30, 2015



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

In accordance with the OMB requirements, later in June 2015, the DHS Under Secretary for Management issued a memorandum to all component heads requiring that they ensure all privileged user accounts under their purview were associated with specific users.⁷ All other accounts not accessed through the use of PIV cards were to be deleted. A comprehensive table of key HSPD-12 milestones and requirements is located at appendix C of this report.

DHS Roles and Responsibilities for HSPD-12 Implementation

In 2007, the DHS Under Secretary for Management assigned the DHS Chief Security Officer (CSO) central responsibility for directing, coordinating, and implementing all HSPD-12 initiatives within the Department.⁸ Additionally, the Office of the Chief Information Officer (OCIO) was to provide technical support and assistance for HSPD-12 implementation. The Office of the CSO (OCSO) established the HSPD-12 program management office (PMO) within its Identity Management Division in June 2009, before renaming and incorporating the office into its Enterprise Security Services Division (ESSD) in 2016.

Subsequent OCSO guidance made responsibility for HSPD-12 implementation more decentralized. Specifically, in December 2008, DHS CSO issued a memorandum to all component CSOs. The memo instructed that they were responsible for managing and executing their respective HSPD-12 implementation plans, and that the headquarters OCSO would only provide guidance for those efforts.⁹ ESSD retained responsibility for PIV card issuance, with DHS component support in staffing and operating the individual PIV Card issuance facilities (PCIF) across the Department.

Further, the Identity Services Branch (ISB), formerly the Credentialing and Access Management (ICAM) group, and part of the Information Sharing Services Office within OCIO, was assigned responsibility for defining IT requirements to support logical access controls. ICAM periodically reported to ESSD managers on headquarters and component PIV card metrics, including the percentage and number of PIV cards issued by credential type (e.g., Federal employee, contractor, or foreign national). General oversight of HSPD-12 implementation was provided through the ICAM Executive Steering Committee, chaired by the DHS CSO and Chief Information Officer (CIO), with voting

⁷ DHS Under Secretary Memorandum, *Immediate Implementation and Reporting of Privileged Users Authentication*, June 25, 2015

⁸ DHS Under Secretary Memorandum, *Implementation Plan Approval Request -Homeland Security Presidential Directive 12*, April 13, 2007

⁹ DHS Chief Security Officer Memorandum, *DHS Component Implementation of Homeland Security Presidential Directive 12*, December 2, 2008



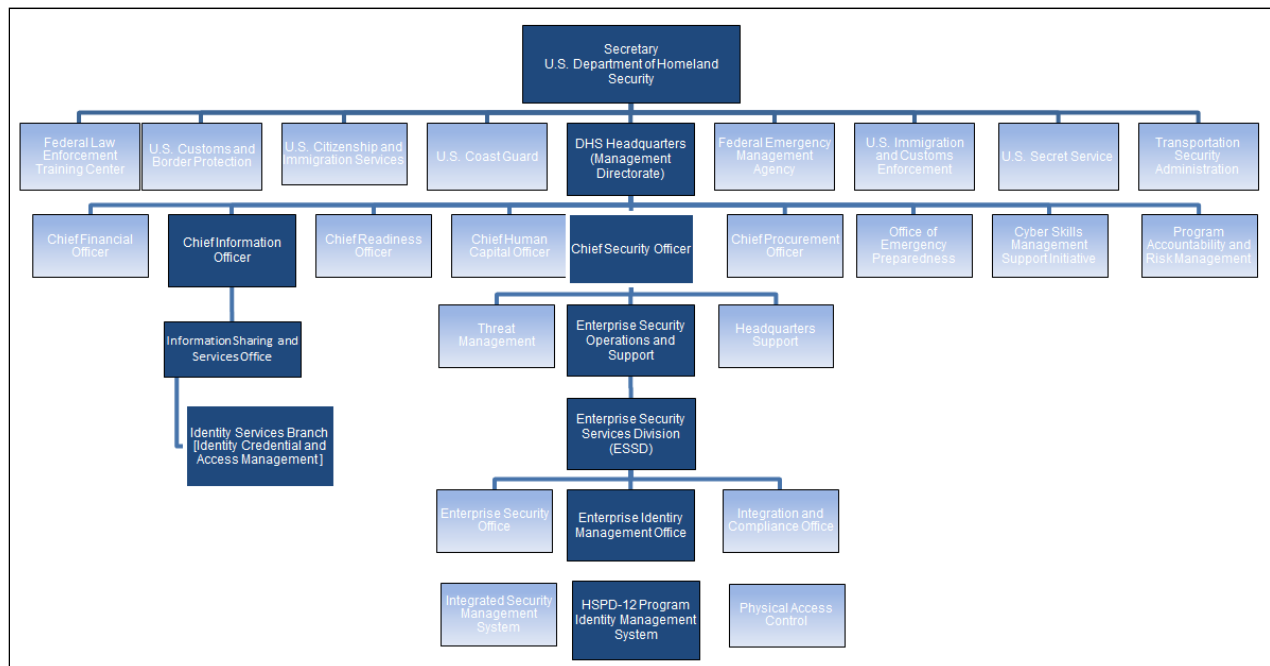
OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

membership from component CSOs and CIOs. This steering committee was developed to provide a venue to collaborate, prioritize, and recommend investment proposals and budgets for ICAM purchases and services related to meeting HSPD-12 requirements.

Figure 3 shows placement of the organizations with primary responsibility for HSPD-12 implementation within DHS.

Figure 3: Key DHS Organizations Responsible for HSPD-12 Implementation



Source: OIG-developed based on DHS OCSO documentation, February 2017

In an effort to expedite HSPD-12 implementation, the DHS Under Secretary for Management issued a memorandum in July 2012 citing metrics for PIV card issuance. Specifically, the target was to require PIV cards to access DHS unclassified networks, with a goal to achieve 50 percent user compliance by the end of fiscal year 2013 and 75 percent by the end of FY 2014.¹⁰

¹⁰ DHS Under Secretary Memorandum, *Implementation of Mandatory Use of the Personal Identity Verification (PIV) Card to Access DHS Networks*, July 31, 2012



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Prior Audit Reports

Prior OIG audit reports published in 2007 and 2010 indicated that DHS had not fully met the requirements of HSPD-12, including implementing an effective process for PIV card issuance. We identified the following issues that prevented the Department from successfully fulfilling HSPD-12 requirements:¹¹

- a lack of priority on implementing the HSPD-12 program;
- inadequate management oversight;
- inadequate funding for HSPD-12 initiatives;
- inadequate resources (i.e., staffing) within the HSPD-12 PMO; and
- the lack of a comprehensive plan for fulfilling the major HSPD-12 requirements—PIV card issuance, physical access controls, and logical access controls.

We conducted this audit to assess DHS' progress in implementing and managing the HSPD-12 program since our prior audits in 2007 and 2010. The scope and methodology for our audit is discussed at appendix A.

Results of Audit

The Department of Homeland Security has not made much progress in implementing and managing requirements of the HSPD-12 program department-wide. Many of the same issues we previously reported in 2007 and 2010 pose challenges today. For example, DHS has an effective process for issuing PIV cards, which is an improvement from the 2010 report. However, it still faces significant program and management challenges in implementing an effective HSPD-12 program, such as placing priority on ensuring termination of the cards for separated contractors who no longer require access.

Further, DHS has made limited progress implementing the controls necessary to regulate access to DHS facilities and systems. At the time of our audit, no DHS component had fully addressed key physical access control requirements, such as inventorying, assigning risk levels, and identifying existing mechanisms for securing owned and leased facilities. This occurred because of insufficient guidance, funding, staffing, and oversight to ensure compliance. Additionally, although DHS components reported 99 percent compliance in

¹¹ *Progress Has Been Made but More Work Remains in Meeting Homeland Security Presidential Directive 12 Requirements* (OIG-08-01), October 2007; and *Resource and Security Issues Hinder DHS Implementation of HSPD-12* (OIG-10-40), January 2010



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

implementing logical access controls on their unclassified information systems, this information had not been independently verified by the Department.

As a result of these deficiencies, DHS cannot ensure that only authorized employees have access to its controlled facilities and systems. The potential remains for individuals who misrepresent their identities to circumvent controls, enter DHS buildings and controlled areas, and cause harm to people and assets. The potential also exists for unauthorized access to information systems, which could result in loss, theft, or misuse of sensitive information.

Effective Process for PIV Card Issuance, but Additional Controls Needed for Card Termination

DHS now has an effective process for issuing PIV cards to all Federal employees and contractors. The Department has also implemented controls to recover PIV cards from separated Federal employees. However, the Department has not placed priority on accounting for the PIV cards issued to contractors who no longer require access to its controlled facilities and information systems. DHS also has not instituted procedures or mechanisms to update facility physical access control systems to deny access related to revoked PIV card credentials.

Subsequent to our audit fieldwork, DHS officials stated they were working to implement a joint OCIO/OCSSO workflow process. This initiative is designed to track logical and physical access to DHS assets by DHS employees and contractors working on behalf of the Department — from onboarding to separation.

Current Process Is Effective for Issuing PIV Cards

More than 10 years since Federal agencies were first required to start implementing HSPD-12, DHS now has an effective process for issuing PIV cards as documented in the *DHS PIV Card Issuer (PCI) Operations Plan*, developed by ESSD, and dated February 2014.¹² The process included:

- Sponsorship and Registration: DHS personnel go through a background investigation initiated within the DHS Integrated Security Management System (ISMS). When personnel meet requirements to obtain a PIV card, ISMS pushes the registration of the individual into the Identity Management

¹² *DHS PIV Card Issuer (PCI) Operations Plan*, issued February 10, 2014, was updated December 23, 2016



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

System (IDMS). A Component Sponsor in the IDMS will sponsor the individual personnel affirming the requirement for a PIV card and provide/validate attributes personalized on the PIV card (e.g., Weapons Bearer, FERRO).

- DHS PIV Card Enrollment: The applicant's identity is authenticated and his or her information is added to IDMS. The applicant appears in person at a PCIF, has his or her identity documents (e.g., passport) scanned into IDMS, and has a photo and fingerprints taken.
- DHS PIV Card Issuance: The applicant's PIN, fingerprints, and certificates are uploaded to the PIV card. The PIV card is printed and issued to the applicant.

Our comparison of these documented processes with FIPS 201 criteria showed alignment with one another. Our observations during fieldwork at two PCIFs affirmed that officials followed these processes for issuing PIV cards to applicants according to Federal standards. Enrollment officials accomplished the registration and enrollment process by verifying the identity of each applicant, scanning identity documents into IDMS, taking digital photographs, capturing biometric (fingerprint) information, and requiring each applicant to select and input a PIN number.¹³

Further, we determined that PIV cards were issued with the minimally required information on the exterior and interior of the cards as outlined in the *PCI Operations Plan*. We observed successful uploading of required electronic information (i.e., cardholder unique identifier, facial image, fingerprint templates, self-selected PIN, and public and private key certificates) from IDMS to the PIV card using a card writer.

From our documentation review, we determined that IDMS and certificate key infrastructure processes were in accordance with FIPS 201 and related guidance. Specifically:

- The Treasury Department and DHS Interconnection Security Agreement, last issued in 2015, detailed the infrastructure for issuing and managing

¹³ Acceptable identity documents as identified in FIPS 201 include an unexpired U.S. passport, U.S. military card, driver's license, or identification card issued by a state or outlying U.S. territory. The identification document must contain a photograph or descriptors such as name, date of birth, gender, height, eye color, and address.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

certificates for PIV cards.¹⁴ (See figure 2, PIV subsystem 1.) DHS used Treasury Department's PKI to issue each PIV card a primary public key certificate, which was then loaded onto the PIV card and used as the primary cardholder authentication mechanism.

- The PKI process outlined in the IDMS system security plan aligned with requirements of the *PCI Operations Plan*.
- The *PCI Operations Plan* detailed how the Treasury PKI and IDMS work together to link PIV card certificates to cardholder identities.

We further verified that the applicant suitability and clearance process, as well as the PIV card issuance process, were incorporated in DHS' employee onboarding process. Specifically, a human resources official (for newly hired Federal employees) or a contracting officer's representative (for new contractors) submits a PIV card request to the PIV card registrar within the respective DHS headquarters or component Personnel Security Division. This action initiates a background investigation of the applicant for suitability prior to granting an entrance-on-duty date.¹⁵ Upon notification from the registrar that the applicant has successfully passed the suitability and background process checks, the human resources official or contracting officer's representative sets the employee's entrance-on-duty date. At that point, the applicant's suitability data is transferred electronically to IDMS, sponsored, and the individual is scheduled for PIV card enrollment.

We affirmed that this process aligned with FIPS 201 requirements for separation of duties among the human resources, enrollment, data entry, and card issuance officials involved in the PIV card issuance process. The separation of duties was required to ensure that no single individual had the capability to issue a PIV card without the cooperation of another authorized person.

HSPD-12 managers indicated they regularly reconciled PIV card issuance with other authorization documentation. For example, they routinely compared the number of PIV cards issued against suitability and credentialing records in DHS' security vetting system of record. This helped verify that all PIV

¹⁴ *Interconnection Security Agreement between the Department of Treasury, Bureau of Public Debt, and Department of Homeland Security Office of the Chief Security Officer and Chief Information Officer*, June 2015

¹⁵ FIPS 201, *Personal Identity Verification of Federal Employees and Contractors*, August 2013, cites the national agency check with written inquiries (or equivalent), as the minimum suitability requirement.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

cardholder's had met the minimum suitability requirements. They also checked PIV card issuance against the revoked user list, which identified all reported damaged, compromised, expired, or otherwise invalid PIV cards. This was to confirm that revoked PIV credentials were no longer active or enabled in the IDMS.

PIV Cards Issued Using this Process

Using this card issuance process, DHS has progressed since program inception to providing PIV cards to 100 percent of the more than 240,000 Federal employees and contractors who need them. DHS officials estimated they issued approximately 107,600 PIV cards to Federal employees and contractors in FY 2016 alone. According to DHS human capital officials, the components are individually responsible for personnel headcounts and no one within DHS centrally tracks the actual numbers of employees and contractors on board. As such, we identified no viable means of comparing total PIV cards issued to total personnel on board within the Department.

Ineffective Process for Collecting the PIV Cards of Separated Contractors

DHS has an effective process for collecting the PIV cards of separated Federal employees, but not for separated contractors. The *PCI Operations Plan* required DHS headquarters and components to implement procedures ensuring that all no longer needed PIV cards were collected, and related access to DHS information systems and facilities was revoked. This was to be done for accountability purposes of rendering the cards inoperable and preventing potential future unauthorized access to facilities and information systems.

We found that prior to being issued a PIV card, each Federal employee or contractor signs a DHS PIV Cardholder Responsibility Agreement, outlining the terms for card use during employment and ultimate surrender of PIV cards that are no longer needed. An HSPD-12 Program Manager stated that, in the event that a PIV card was expiring and needs renewal, DHS uses a combination of automated and manual processes to notify employees of impending revocation of the cards. As part of those processes, IDMS sends an email notification to the cardholder indicating that the Federal employee's PIV card is close to expiration. The email instructs the cardholder to contact the respective security office to schedule a PIV card appointment. However, when employment or association with DHS is terminated or appointment to the position indicated on the card is discontinued, the cardholder must surrender his or her PIV card to the appropriate authority (e.g., supervisor or contracting officer's representative). PIV cards that are no longer needed should be returned to a



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

PCIF and the credential revoked. Field locations can destroy PIV cards once revocation has been confirmed.

Further, DHS had a sound process for collecting the PIV cards of separated Federal employees. Specifically, this process entails a separated Federal employee surrendering his or her PIV card to the component security office as part of the out-processing process. A security officer then logs into IDMS, revokes the card's credentials, and destroys the card. If the security officer does not have access to IDMS, the officer mails or hand-delivers the PIV card to a PCIF for revocation of the credentials and destruction of the card. If the Federal employee's PIV card is reported lost or stolen at the time of the employee's separation, the card's credentials are simply revoked.

However, managers at three PCIFs stated that DHS had no consistent process in place to collect PIV cards for separated contractors. As such, a number of PIV cards for separated contractors were not properly accounted for and remained in possession of the contracting officer representative (COR) rather than being returned to the cardholder's PCIF to have the credentials revoked. In other instances, even though PIV card credentials were revoked, the PIV card remained in the possession of the contractor after termination.

According to ESSD officials, DHS has not instituted an automated capability to alert HSPD-12 officials of the need to deactivate PIV cards for separated contractors, similar to what was in place for Federal employees. The Department revoked 91,680 PIV cards in FY 2016. Of those, 24 percent (22,029) were contractor PIV cards. However, this number only represented the number of contractor PIV cards collected and expired. Given the lack of accountability for all contractor cards, the actual number could be higher.

One program manager explained that contractor data, such as contract period of performance or contract employee off-boarding, were not centrally tracked. If available, such information could be used to determine when the contractor's access to DHS facilities and information systems should be revoked. ESSD officials had met with DHS Chief Procurement Office representatives and found that this information was not captured. Instead, CORs were left to independently manage the start and end dates for their contractors. CORs from headquarters, U.S. Immigration and Customs Enforcement (ICE), and U.S. Citizenship and Immigration Services (USCIS) told us that the number of contractors they were responsible for at any given time could be several hundred, making it difficult to keep account of this information.

DHS also had not put procedures or mechanisms in place to update access control systems and deny access to individuals possessing PIV cards for which



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

credentials had been revoked. Effective procedures or mechanisms were needed to ensure that, in the event that the PIV cards of separated employees were not collected, the cards could not be used for unauthorized access to DHS facilities or systems. For example, there was no central or automated means of alerting guards at facilities department-wide that certain individuals should no longer be admitted. This was especially needed in locations where an individual could use a revoked PIV-card as a “flash pass,” enter a building, and gain unauthorized access to employees, controlled areas, systems, and property.

Physical and Logical Access Controls Were Not Fully Implemented in Compliance with HSPD-12 Requirements

DHS had not fully implemented required physical and logical access controls for all headquarters and component facilities and systems. Unlike the centralized management approach to PIV card issuance, a decentralized approach was used for ensuring physical access controls (PACS). That is, each headquarters or component security office was responsible for implementing its respective control mechanisms and reporting on progress. However, none of the security offices we evaluated had fully implemented the physical controls necessary to regulate access to their owned and leased facilities and controlled areas within those facilities. Further, components reported implementing approximately 99 percent of the logical access controls required for DHS’ unclassified information systems through FISMA reporting; however, those numbers were self-reported and not independently verified for accuracy and completeness by DHS.

Physical Access Control Systems Not Fully Implemented

Key requirements for implementing PACS at owned and leased facilities included inventorying facilities, identifying facility security levels, assessing existing mechanisms for securing facilities, and reporting on progress made. We found, however, that DHS headquarters and components had made limited progress in fulfilling these PACS requirements in their respective organizations. Causes for the lack of progress included insufficient guidance, funding, staffing, and inadequate oversight to ensure compliance.

Key PACS Implementation Requirements

An HSPD-12 compliant PACS is designed to regulate the ability of an employee or contractor using a PIV card to access a facility or a controlled area within a facility. To be fully compliant, the PACS must be able to authenticate each PIV



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

cardholder's identity and then determine whether the cardholder has authorized access.

In November 2012, the DHS CSO directed the Headquarters Physical Security Division and component CSOs to participate in developing a department-wide implementation strategy and modernization plan to meet these PACS requirements.¹⁶ The resulting strategy document indicated that each CSO across the Department would provide the scope, schedule, and budget the component would need to fully utilize PIV cards as the basis for authorizing facility access. To assist the OCSO in accurately estimating all requirements and costs, components were to address four key elements in PACS implementation: inventorying facilities, identifying facility security levels, pinpointing existing mechanisms for securing facilities, and quarterly reporting on progress made.

Limited Progress in PACS Implementation

Our audit showed that DHS components did not adequately fulfill requirements for PACS implementation in the four key areas. Each area is discussed in the following paragraphs.

Facility Inventories

The DHS PACS modernization plan required that the security offices of nine major DHS components provide complete inventories of their DHS-owned and leased facilities. These inventories were needed to determine facility security levels and the mechanisms needed to control access to each facility. ESSD sent a facility inventory request to following nine major DHS entities.

- DHS headquarters
- Federal Emergency Management Agency (FEMA)
- Federal Law Enforcement Training Centers (FLETC)
- ICE
- USCIS
- U.S. Customs and Border Protection (CBP)
- Transportation Security Agency (TSA)
- United States Coast Guard
- United States Secret Service

¹⁶ *DHS Modernization Strategy for Physical Access Control Systems (PACS)*, September 6, 2012



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Although all of the DHS component security offices responded to the facility inventory requirement, ESSD officials placed little or no confidence in their responses for two primary reasons. First, all of the reporting security offices had not uniformly defined and identified what constituted a facility. For example, FLETC security managers reported having 4 facilities, but identified 323 buildings at just 1 of those locations. Similarly, CBP managers indicated that a single facility consisted of 19 buildings.

Second, none of the component inventories were independently validated for accuracy and completeness. Rather, ESSD accepted the numbers reported by the component security offices at face value. To the extent that the inventories are not accurate, all controlled facilities may not be accounted for so that adequate measures can be applied to protect property, resources, and people.

Facility Security Levels

The *Interagency Security Council Physical Security Standards* required DHS component organizations to make facility security level (FSL) determinations for their owned or leased facilities.¹⁷ DHS Instruction Manual 121-01-010, *Physical Security*, established the use of risk assessments for making these determinations and identifying corresponding requirements for PACS implementation at each facility.¹⁸ Per the PACS modernization plan, each DHS organization was to provide the FSL determination to ESSD for review and oversight.

Determining an FSL entailed considering factors that could make the facility a target for adversarial acts (threats), as well as characterizing the value or criticality of the asset (consequences). FSL determinations could range from Level I (lowest risk) to Level V (highest risk), depending on the following factors:

- Mission criticality: Importance of the missions carried out by tenants in the facility (e.g., ports of entry and communications facilities).
- Symbolism: Attractiveness of the facility as a target based on well-known operations indicating it is a government facility (e.g., popular tourist destination and executive department headquarters).
- Facility population: Peak number of personnel in the government space, including employees and visitors, if the population is part of normal business operations (e.g., small office or international trade center).

¹⁷ Interagency Security Committee, *The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard*, August 2013

¹⁸ DHS Instruction Manual 121-01-010, Revision #01, *Physical Security*, July, 21, 2014



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

- Facility size: Square footage of all federally-occupied space in the facility.
- Perceived threat to tenant agencies: Attractiveness of the facility as a target, due to the nature of public contact, conduct of business, or history of adversarial acts committed at the facility (e.g., criminal and bankruptcy courts, and high-risk law enforcement facilities).

The methodology for assessing and scoring facilities based on these factors is reflected in table 1.

Table 1: Methodology for Determining FSLs

Facility Security Levels	1	2	3	4
Mission Criticality	Low	Medium	High	Very High
Symbolism	Low	Medium	High	Very High
Facility Population	< 100	101-250	251-750	> 750
Facility Size (Square feet)	< 10,000	10,000 – 100,000	100,001-250,000	>250,000
Perceived Threat to Tenant Agencies	Low	Medium	High	Very High
Facility Security Levels (FSLs)	I 5-7 points	II 8-12 points	III 13-17 points	IV 18-20 points

Source: Interagency Security Committee Standard, *Facility Security Level Determinations for Federal Facilities*, August 2013

Using this methodology, an FSL decision-making authority was to assign a point value for each factor listed in the first column of the table. The FSL rating was determined by the total number of points. The decision-making authority could adjust the FSL rating up or down by one level based on additional, discretionary factors such as impact on infrastructure or costs associated with facility alterations.

Despite this requirement, only the FLETC and USCIS security offices met the requirement in 2014 to submit to ESSD an FSL for all of their reported facilities. The security offices for DHS headquarters, Secret Service, and Coast Guard submitted no FSLs. Further, the Coast Guard provided a memorandum to the CSO indicating that it used the Department of Defense Common Access Card, instead of the PIV card, for identity verification as well as physical and logical access to its military facilities and systems.¹⁹ A Coast Guard official stated that DHS-owned and leased facilities and information systems are not

¹⁹ The Defense Common Access Card is used by the Coast Guard employees for identification and access to Department of Defense controlled facilities and systems.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

currently compatible with the Defense Common Access Card system. As such, CSO accepted this Coast Guard decision. CSO officials stated that at the current time, there is no timeframe to implement a joint solution for Coast Guard officials to access both military and DHS facilities and systems.

Per figure 4, the remaining four of nine DHS components' security offices provided FSL determinations for some, but not all, of their reported facilities. Figure 4 provides a tally of each component's reported facilities, the number with FSLs, and the percent compliance.

Figure 4: Reported Numbers of Component and Headquarters FSLs

Component	Reported number of facilities	Reported number of facilities with an FSL rating	Percent compliance
FLETC	4	4	100%
USCIS	139	139	100%
FEMA	92	83	90.2%
ICE	394	237	60.2%
CBP	823	105	12.8%
TSA	673	39	5.8%
DHS HQ	29	0	0%
Secret Service	168	0	0%
Coast Guard	437	0	0%
Total	2,759	607	22.0%

Source: FSL numbers reported to ESSD in 2014

As shown, component security offices reported to ESSD that about 22 percent (607 out of 2,759) of the reported facilities in 2014 had FSL ratings. During our audit fieldwork in spring 2017, ESSD officials indicated that these numbers had not changed. Lacking such ratings, DHS had no effective means of ensuring the proper controls were in place commensurate with the risk of unauthorized physical access to its facilities.

Existing Controls for Securing Facilities

The PACS modernization plan required that each DHS component security office provide ESSD with an assessment of the component's progress in implementing a PACS at each of its owned and leased facilities. The PACs implementation assessment was to provide the total number of controlled facilities, the existing PACS mechanisms in each facility, and the additional



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

equipment needed to satisfy HSPD-12 objectives. PACS equipment might consist of:

- card readers to read the information stored on the PIV card of the user seeking access at a facility,
- databases that receive the information transmitted from the card reader and sent to IDMS to authenticate the user, and
- controllers that check the PACS authorization system to verify that the user is authorized access to the facility.

Figure 5 depicts the interaction among these key PACS elements.

Figure 5: Reported Numbers of Headquarters and Component Progress

Component	Reported number of facilities	Reported number of facilities requiring PACS	Difference
CBP	823	846	23
FLETC	4	4	0
DHS HQ	29	29	0
USCIS	139	137	-2
FEMA	92	81	-11
ICE	394	236	-158
Secret Service	168	0	-168
Coast Guard	437	0	-437
TSA	673	82	-591

Source: PACS progress reported to ESSD in 2014

As shown in figure 5, only CBP, FLETC, and DHS headquarters met the requirement to report on PACS implementation progress at each of its controlled facilities. CBP incorrectly reported more operational PACS than the number of reported facilities. CBP included additional operational areas.

According to FEMA, the Coast Guard, and TSA, not all of their facilities required PACS. The Secret Service and Coast Guard PACS implementation plans, dated October 2014 and November 2014 respectively, indicated no PACS were needed at any of their facilities. Further, all component submittals failed to provide the number of facility access points requiring PACS. Identification of the access points was needed to determine the number and type of PIV card readers, as well as the number of databases and controllers required to authenticate PIV card users and authorize facility access.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

The wide disparity in reporting on PACS implementation progress indicated a lack of component security office understanding of the requirement or a failure to conduct the assessments needed to address the reporting requirement. ESSD officials placed little or no confidence in the responses provided by headquarters and component security offices since the results were not independently validated for accuracy and completeness. ESSD also did not follow up.

Reporting on PACS Implementation Progress

The PACS modernization plan required that DHS components quarterly report their PACS implementation status to the DHS OCSO. This included providing a milestone date for each of the three PACS implementation phases defined in the plan.

- Phase 1: Planning, included defining requirements, determining as-is landscape and developing a technical, organizational, and management approach to implementing PACS.
- Phase 2: PACS capabilities, included establishing the PIV card as the basis for facility access, connections for PIV authentications, and prioritizing upgrades to PACS.
- Phase 3: Enhanced PACS services and interoperability, included upgrading facilities until complete, accepting other agency PIV Cards, and achieving interoperability with external systems as needed.

In 2014, only DHS headquarters, CBP, FEMA, FLETC, and ICE complied with the requirement to provide milestone dates for completing each phase. That same year, USCIS provided a milestone date for only completing phase 1. TSA and Secret Service provided no milestone dates for any of the three phases. During our audit, OCSO managers indicated that none of the component security offices had provided quarterly reporting on their PACS implementation progress since these initial results were received in 2014.

Causes for Lack of PACS Implementation Progress

The lack of headquarters and component organization progress in implementing PACS can be attributed to a lack of priority for HSPD-12 implementation. We found some of the same issues we previously reported in 2007 and 2010: insufficient guidance, funding, staffing, and oversight.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Insufficient Guidance

The PACS modernization plan did not provide all of the guidance necessary for headquarters and component security managers to successfully complete PACS implementation in a timely manner. For example, although the strategy required components to report their respective totals of owned or leased facilities, it did not clearly define what constituted a facility in order for them to accurately and consistently comply. That can account for FLETC security managers reporting four facilities but identifying more than 300 buildings for just one of those locations.

DHS had no subject matter expert in place to assist its components in addressing requirements of the PACS modernization plan. DHS previously had such a representative in place after the plan was issued in November 2012, but this individual departed from DHS after a few months and was never replaced. DHS also did not reach out to components to offer help in spurring PACS implementation progress after the initial guidance was first released.

Although DHS had a process for component CSOs to escalate issues or request help in developing PACS requirements for their respective facilities, this process was not utilized by all component CSOs. For example, component security managers encountered difficulty upgrading existing PACS to meet HSPD-12 PIV authentication requirements lacking guidance from ESSD on how and where to direct questions for addressing these issues. Other difficulties included making modifications to facilities to accommodate PACS equipment, such as card readers and the wiring needed to connect them to PACS servers.

Insufficient Funding

In 2010, we reported that HSPD-12 was an unfunded mandate and not a departmental priority. As such, available funding was often diverted to higher priority programs. In 2015, DHS placed emphasis on issuing PIV cards, which was funded through a working capital fund with component costs apportioned by the percentage of PIV cards they issued. However, fulfilling HSPD-12 physical access control requirements remained an unfunded mandate whose costs were borne by DHS headquarters and components. PACS implementation competed with other component priorities and, as a result, components were often reluctant to fund these activities.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Insufficient Staffing

HSPD-12 managers had inadequate staff resources to assist headquarters and component managers in fulfilling their PACS implementation requirements and verifying the results. ESSD support for PACS implementation consisted of one manager responsible for providing guidance and assistance to component organizations department-wide. The ESSD manager cited this as the primary reason why he was unable to verify PACS requirements submitted by component security offices for accuracy and completeness. Further, some component security offices assigned their employees other primary duties in addition to responsibility for PACS implementation. For example, two employees from the DHS Headquarters Security Office Physical Security Division were assigned PACS implementation duties but also were responsible for other IT operations and security priorities that occupied all of their time.

Inadequate Oversight

As previously discussed, DHS shifted in 2008 from a centralized to a decentralized approach to HSPD-12 implementation, leaving each component responsible for its own HSPD-12 compliance. ESSD retained the role of providing PACS implementation guidance as needed to component security offices, but it had no oversight and enforcement authority. The PACS modernization plan issued by ESSD outlined specific component reporting requirements (e.g., number of facilities, an FSL rating for each facility, and an inventory of any PACS systems) for determining the equipment and associated costs needed to meet HSPD-12 objectives. However, it specified no ESSD oversight process to verify the reported information for completeness and accuracy. This lack of oversight also resulted in ESSD receiving required reports almost 2 years after they were requested.

Although the PACS implementation strategy required component CSOs to develop project schedules with proposed start and end dates, control gates, and milestones for ensuring PACS implementation remained on schedule, ESSD neither tracked nor updated these project schedules. ESSD officials stated that from October 2014 until November 2016, there were no efforts to update the components' lists of requirements or to assess their progress in implementing PACS. Given the lack of oversight and tracking, officials we interviewed in May 2017 cited little to no change in department-wide progress in implementing PACS since initial submission of their modernization plans in 2014.

We found confusion regarding the responsibility for FSL assessments of DHS facilities. ESSD officials believed this was entirely the responsibility of the



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Federal Protective Service (FPS), but FPS personnel stated that they were only responsible for FSL assessments of General Services Administration-leased buildings and DHS-owned properties with an established Service Work Agreement between FPS and the facility owner. We ultimately determined that, according to DHS Instruction Manual 121-01-010-01, *Physical Security, revision 1*, each component CSO was responsible for maintaining a current real property inventory that includes FSL designations. Nonetheless, the OCSO did not routinely receive FSL assessments from component CSOs and FPS so that it could carry out its HSPD-12 mandated responsibility for ensuring that every DHS facility had an FSL rating.

Ultimately, this lack of oversight meant there was no established process for review and approval of all component PACS expenditures to ensure they were HSPD-12 compliant. The *DHS Acquisition Manual* requires that the PMO review all HSPD-12 products and services prior to procurement through the General Services Administration Federal Supply Schedule 70 or through open market acquisitions.²⁰ PACS-related procurements were required to be coordinated through the PMO prior to securing funding, but this did not occur on a consistent basis.²¹ For example, one PMO manager mentioned receiving only one request to review a PACS equipment requisition since June 2015. CSO officials cited issues with components purchasing PACS equipment that was not compatible with the General Services Administration-approved list. To illustrate, CBP officials stated they had purchased 203 different types of PACS equipment from various manufacturers, along with 185 disparate software versions to support them. Similarly, FEMA officials discussed incompatibility issues with two HSPD-12 compliant card readers purchased from different vendors.

Without an effective acquisition review and approval process, there was a lack of visibility and accountability regarding the PACS equipment acquired and implemented department-wide. As such, there was no way to ensure that all PACS equipment purchases (i.e., card readers, scanners, servers) complied with HSPD-12 while meeting the operational and security needs of the stakeholder.

Required Logical Access Controls Not Fully Implemented

Not all required logical access controls for DHS component information systems were implemented per Federal standards. For example, HSPD-12

²⁰ *DHS Acquisition Manual*, October 2009

²¹ *DHS Modernization Strategy for Physical Access Control Systems (PACS)*, September 6, 2012



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

program officials could not confirm that risk assessments were conducted to determine what IT security controls were needed as a prelude to Logical Access Control System (LACS) implementation. We identified several information systems that were not PIV-enabled and therefore not in compliance with HSPD-12 requirements. Further, DHS reported 99 percent compliance in LACS implementation; however, those numbers were self-reported by components and never verified for accuracy and completeness.

Risk Impact Assessments Not Always Conducted to Support LACS Implementation

System risk impact assessments and commensurate IT controls were not implemented as required as a prelude to instituting logical access controls directed by HSPD-12. Logical access involves the use of a credential to control access to a computer, network, or location on a network.

In 2005, OMB directed Federal agencies to assess the extent to which their respective information systems should be protected based on potential risk impact.²² Agencies were directed to use FIPS 199 as a guide and assign a risk impact level (low, moderate, or high) to each information system, depending on the possible magnitude of harm to operations, assets, or individuals through the loss, theft, or misuse of information.²³ Risk assessment ratings determine potential risk impact based on —

- inconvenience, distress, or damage to standing or reputation;
- financial loss or agency liability;
- harm to agency programs or public interests;
- unauthorized release of sensitive information;
- personal safety; and
- civil or criminal violations.

Despite these requirements, DHS did not assign a risk impact level to all unclassified information systems. Our FY 2016 FISMA evaluation showed that DHS did not always follow FIPS 199 policies. We reported that 3 of 10 system security authorization packages and supporting documentation did not adequately address risk impact levels, as they improperly categorized risk or had missing information.

²² OMB M-05-24, Memorandum For The Heads Of All Departments and Agencies, *Implementation of Homeland Security Presidential Directive (HSPD)12 – Policy for a Common Identification Standard for Federal Employees and Contractors*, August 5, 2005

²³ NIST FIPS 199, *Personal Identity Verification of Federal Employees and Contractors, Version 2*, February 2004



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Not All Unclassified Information Systems Were PIV-enabled

HSPD-12 requires PIV-enablement of all unclassified information systems. Exceptions to this requirement are only granted under extenuating circumstances, such as when an information system is being decommissioned. To the extent that the Department's unclassified systems are PIV-enabled, a justification and waiver must be in place to maintain an authority to operate that system.

Despite these requirements, we identified 41 sensitive systems at Science and Technology used for explosive detection and radioactive material research that were not PIV-enabled and had no waiver to maintain an authority to operate. When alerted, the Science and Technology Chief Information Security Officer indicated that steps were being taken to move the standalone computers onto a network that requires PIV authentication.

Component Reporting on Logical Access Controls Was Not Verified

ICAM managers could not confirm that all DHS unclassified systems were PIV-enabled because they relied on component reporting and did not verify those numbers for accuracy and completeness. Chief Information Security Office (CISO) officials said a lack of resources prevented them from carrying out key HSPD-12 related duties such as:

- reconciling and ensuring accurate inventories of IT assets across the Department;
- independently verifying that all unclassified information systems were assessed and had risk impact ratings per FIPS 199; and
- ensuring all Department legacy systems were PIV-enabled, logical access controls were present on DHS unclassified information systems, and waivers were granted for extenuating circumstances.

In part, ICAM managers attributed their reliance on component-reported HSPD-12 compliance information to shortages in funding. As previously stated, HSPD-12 remained an unfunded mandate requiring that the costs for LACS implementation be borne by DHS components, just like for its PACS counterpart. In some cases, components had to postpone HSPD-12 implementation activities due to lack of funding. For example, in FY 2016, TSA deferred its LACS implementation for some of its IT systems when funding was reprogrammed towards updating or replacing an aging and obsolete IT infrastructure, which was considered a higher priority. In other cases, components funded LACS implementation through existing component



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

initiatives. To illustrate, in FY 2016, FEMA reprogrammed approximately \$174,000 from its CSO in order to further LACS implementation. This adversely affected the ability of its Fraud and Internal Investigations unit to accomplish its investigations and enforcement mission to protect FEMA personnel and assets. Similarly, CBP redirected approximately \$2 million in operations funding from its IT modernization effort in order to further LACS implementation. This resulted in delays in replacing legacy systems and upgrading its aging and obsolete network infrastructure.

Further, ICAM officials said they had inadequate staff to conduct oversight needed to ensure department-wide HSPD-12 compliance. Staffing this activity was not a priority and efforts to obtain contractor support to fill the gap in FY 2017 also were not successful. One DHS official stated that it would be useful to have an automated process in place to help ensure accuracy and completeness of DHS information system inventories. Other DHS officials anticipated that the Continuous Diagnostics and Mitigation initiative would provide “real-time” identification of information systems, including the security posture of each.²⁴ However, CISO officials could not provide a timeframe for implementing this capability.

Lastly, a CISO official stated that specialized training had been available in the past for system owners and information system security officers on properly documenting and validating system security plans, conducting risk assessments, and addressing system deficiencies in the plan of actions and milestones. However, this training was no longer included in the DHS CIO’s budget, although it was still needed to help identify controls needed to implement LACS in compliance with HSPD-12. Therefore, the CISO relied on components to ensure that role-based training was accomplished.

Challenges to HSPD-12 Program Management Pose Risks to Personnel, Property, and Information

DHS shortfalls in complying with all requirements of HSPD-12 present risks for staff, facilities, and data department-wide. Lacking an effective process to account for the PIV cards of separated contractors, DHS cannot prevent prohibited use of the cards to misrepresent identity and circumvent physical and logical access controls. To the extent that the cards go uncollected and credentials are not revoked, the potential remains for unauthorized individuals

²⁴ In relative terms, “real time” refers to the ability to determine a snapshot of a system’s status.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

to use them to enter DHS buildings and controlled areas, access information systems, and cause harm to people and assets.

For example, in November 2016, a DHS contractor was separated from employment and the individual's PIV card was never collected and permissions were not removed from the PACS and LACS systems at DHS headquarters. As a result, the employee entered the complex on multiple occasions and accessed information systems within a Sensitive Compartmented Information Facility. The contractor continued to have unfettered access to this classified area for more than 3 months until the situation was discovered and remedied in March 2017 when the contractor applied for a Joint Worldwide Intelligence Communications System account with access to classified information. Upon review of the application, a headquarters security officer concluded that the contractor had separated from the agency on November 29, 2016, the previous year. As such, the classified system access request was denied and the HSPD-12 badging office was notified of the situation.²⁵

In general, systems without PIV-enablement also increase the opportunity for breaches of controlled information. One such breach occurred in July 2014, when a former employee of another Federal agency pled guilty to accessing Government servers that hosted a website used to support mortgage loan modification programs. The employee was terminated from his position in August 2013. However, using an administrator account and password that he had retained, this individual was able to repeatedly log onto Government servers and make unauthorized changes to website functionality. This breach was estimated to be as much as \$70,000 in website repairs; however, to the extent that losses of revenue and mission-critical information also resulted, the impact was likely much more extensive.

DHS has much work to do to fully implement HSPD-12 requirements and prevent future such incidents from occurring within the Department. Taking corrective actions to secure DHS' controlled facilities and systems is important, especially given its homeland security mission and the need to protect the public trust in carrying it out. Until DHS can accurately account for all PIV cards, identify all of its facility holdings and their security requirements, and fully implement required physical and logical access controls, the vulnerabilities will remain. DHS must make HSPD-12 a priority, but to do so, leadership must recognize the risks involved and adequately support the efforts

²⁵ Memorandum from the Director of the DHS Headquarters Security Services Division, *Subject: Notice Letter of Infraction - SSPD 17-30-MGMT*, dated April 11, 2017



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

of those tasked with its implementation. Only then can DHS be positioned to address the deficiencies we identified in this report.

Recommendations

We recommend that the DHS Chief Security Officer:

Recommendation 1: Develop and implement a process to collect, revoke, deactivate, and destroy the PIV cards of all contractors who no longer require access to DHS facilities or systems.

Recommendation 2: Develop and implement a plan for ensuring the removal of facility and information system access for all PIV cards after their credentials are revoked.

Recommendation 3: Develop and implement a plan for providing sufficient guidance, funding, staffing, and oversight for procuring and implementing PACS department-wide.

Recommendation 4: Implement a plan for ensuring that DHS components inventory their facilities, identify facility security levels, pinpoint existing mechanisms for securing facilities, and quarterly report to the OCSO on progress made, to assist in accurately estimating the requirements and costs of PACS implementation.

Recommendation 5: Coordinate with the CIO on ensuring that components conduct valid and current risk assessments for information systems under their purview as a means of identifying requirements for logical access control systems implementation.

Recommendation 6: Coordinate with the CIO on ensuring that components PIV enable all unclassified information systems under their purview.

Recommendation 7: Develop and implement a process for ensuring verification and validation of all component reporting to OCSO on their activities to meet HSPD-12 requirements.

OIG Analysis of Management Response to Recommendations

We obtained management comments to the draft report recommendations from the Director of the Departmental GAO-OIG Liaison Office. We included a copy of those comments, in their entirety, in appendix B.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

The Department concurred with all 7 recommendations. Below is a summary of their management response to each recommendation and our analysis of their proposed corrective action plan.

Recommendation 1: Develop and implement a process to collect, revoke, deactivate, and destroy the PIV cards of all contractors that no longer require access to DHS facilities or systems.

Management Response

Concur. Management noted that DHS OCSO staff brought this requirement to OIG's attention as it is a known challenge for which the HSPD-12 Program already has a mitigation plan in place. Successfully implementing this recommendation requires a mechanism to track, manage, and inform the HSPD-12 Program when a contractor is off boarding. Management indicated the DHS PIV Card Issuer Operations Plan exists today to provide the process for collecting, deactivating, and destroying PIV cards of all contractors and DHS is working to improve its monitoring of these processes. In addition, DHS OCSO staff continues to work with the DHS OCIO's Access Lifecycle Management (ALM) Project Team to address this recommendation. Specifically, ALM is being implemented to manage the lifecycle of access for employees and contractors at DHS. This will improve the Department's ability to identify active contractors by:

- identifying who is on a contract at any time,
- off boarding a contractor at any time,
- off boarding contractors based on contract expiration, and
- certifying quarterly that contractors on task orders are still required.

Management indicated each of these processes can result in off boarding from DHS, including removal of logical (information technology) access, physical access, notification to the Federal point of contact to collect the PIV card, and automated inactivation of the PIV card. Management expected the ALM pilot at DHS Headquarters to be completed by March 31, 2018, with expansion to the Management Directorate in the fourth quarter of FY 2018. At that point, ALM will provide an enterprise service to components to help address this same challenge. Management requested that OIG consider this recommendation open and resolved pending completion of the aforementioned activities, estimated for September 30, 2018.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

OIG Analysis

We believe the actions described satisfy the intent of this recommendation. This recommendation will remain open and resolved until the Department provides documentation to substantiate that planned corrective actions are completed to implement a process to collect, revoke, deactivate, and destroy PIV cards of all contractors that no longer require access to DHS facilities or systems.

Recommendation 2: Develop and implement a plan that removes facility and information system access for all PIV cards after their credentials are revoked.

Management Response

Concur. DHS has established a project to automate the provisioning and de-provisioning of system and facility access through the ALM solution. ALM integrates with DHS information technology and establishes capabilities to remove system and facility access when the corresponding PIV card is revoked. OCSO and OCIO will continue deployment of ALM and revise plans accordingly until integration with LACS and PACS is complete. OCSO, in cooperation with OCIO, will also work with DHS components to establish corresponding policies and procedures, as needed. Management requested that OIG consider this recommendation open and resolved pending completion of the aforementioned activities, estimated for September 30, 2018.

OIG Analysis

We believe that the actions described satisfy the intent of this recommendation. This recommendation will remain open and resolved until the Department provides documentation to support that planned corrective actions are completed to remove facility and information system access for all PIV cards after their credentials are revoked.

Recommendation 3: Develop and implement a plan for providing sufficient guidance, funding, staffing, and oversight for procuring and implementing PACS Department-wide.

Management Response

Concur. Management indicated that, in order to address development and implementation of the PACS Modernization Strategy, OCSO will author and implement a plan for providing sufficient guidance, funding, staffing, and oversight for procuring and implementing PACS department wide. The majority



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

of PACS assets operated within the Department at the current time do not fully support its ability to implement the use of PIV and PKI. Most assets will require some form of hardware and software upgrades or replacement. The activities needed to address these issues are already underway through the current DHS PACS Modernization effort. An Integrated Project Team has been convened to look at challenges or constraints that may be encountered during PACS Modernization implementation. The Integrated Project Team assessed the current capability, generating findings as a gap analysis. The gap analysis will be used to develop a Capability Assessment Report (per the DHS Joint Requirements Council process), including a series of recommendations such as non-material change requests in the form of physical access control policy updates, audit/oversight functions, cost estimation capability, and options for DHS senior leadership to consider to achieve full Federal ICAM compliance. Management requested that OIG consider this recommendation open and resolved pending completion of the aforementioned activities, estimated for September 30, 2018.

OIG Analysis

We believe that the actions described satisfy the intent of this recommendation. This recommendation will remain open and resolved until the Department provides documentation to support that planned corrective actions are completed to develop and implement sufficient guidance, funding, staffing, and oversight for procuring and implementing PACS Department-wide.

Recommendation 4: Implement a plan that confirms that DHS components inventory their facilities, identify facility security levels, pinpoint existing mechanisms for securing facilities, and quarterly report to the OCSO on progress made, to assist in accurately estimating the requirements and costs of PACS implementation.

Management Response

Concur. Management indicated that a PACS Reporting Tool has already been developed. A pilot release with DHS Headquarters, FEMA, and FLETC began on January 8, 2018, and will be expanded to the other components in the third quarter of FY 2018. This tool was developed to identify all DHS-occupied facilities, associated facility security level designations, and detailed information on currently used PACS assets. The information will be used to support OCSO/OCIO tracking of PACS, authorization to operate, and use of approved products on the GSA-Approved Products List for quarterly reporting. Additionally, the catalogued information will be used to monitor component



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

progress in achieving PACS Modernization. The reporting tool is being coordinated with the DHS Office of the Chief Readiness Support Officer to build upon known facility information. Data analytics will be developed by OCSO and used with facility data to plan physical access control systems implementation requirements and cost estimates. Management requested that OIG consider this recommendation open and resolved pending completion of the aforementioned activities, estimated for September 30, 2018.

OIG Analysis

We believe that the actions described satisfy the intent of this recommendation. This recommendation will remain open and resolved until the Department provides documentation to support that the planned corrective actions are completed.

Recommendation 5: Coordinate with the CIO on ensuring that components conduct valid and current risk assessments for information systems under their purview as a means of identifying requirements for logical access control systems implementation.

Management Response

Concur. The DHS OCSO and DHS OCIO will coordinate HSPD-12 implementation as it pertains to risk assessments for information systems. Management asserted the DHS OCIO's Office of the Chief Information Security Officer has had policies, procedures, and a process in place preceding, during, and subsequent to this audit to hold components accountable for conducting risk assessments for the unclassified information systems under their purview. For example, the DHS CISO's office requires that, in accordance with *DHS Sensitive Systems Policy Directive 4300A*, risk assessments be conducted as part of the systems assessment and authorization process. Implemented through required use of the DHS automated Information Assurance Compliance System, the process: 1) does not allow components to progress through the authorization steps until the risk assessment is completed, and 2) requires the component CISO or equivalent to confirm that the risk assessment is valid, complete, and current. The tool uses the results of the assessment to generate the required security controls baseline, including the LACS, to be implemented by the component system. Risk assessments for component systems are also required to be updated or revised when the system authorization to operate is refreshed or according to other policy requirements for specialized systems. Component CISOs are permitted by NIST and DHS policy to tailor controls based on their environments and mission



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

requirements. Management requested that OIG consider this recommendation resolved and closed.

OIG Analysis

We believe that the actions described satisfy the intent of this recommendation, since mechanisms are in place for components to conduct valid and current risk assessments for information systems under their purview. This recommendation will be considered resolved and closed.

Recommendation 6: Coordinate with the CIO on ensuring that components PIV-enable all unclassified information systems under their purview.

Management Response

Concur. Management indicated that the DHS OCSO and DHS OCIO will coordinate HSPD-12 implementation as it pertains to PIV-enablement of all unclassified information systems. The DHS OCIO has had a process in place to hold components accountable for PIV-enabling unclassified information systems for which the components are responsible. *DHS Sensitive Systems Policy Directive 4300A* requires the use of PIV credentials to access existing and new systems. The policy directive was changed pursuant to the DHS Under Secretary of Management's issuance of a memorandum, *Strengthening DHS Cyber Defenses*, on July 22, 2015. The policy directive states that system owners are responsible for successful operation of information systems and programs within their program areas, and ultimately are accountable for their security. Further, system owners ensure information security compliance, development, and maintenance of security plans, user security training. They also notify officials of the need for security authorization and resources.

The DHS OCIO uses its risk management process to hold components accountable for PIV-enabling its unclassified information systems. The process is required by the 4300A policy, defined in the *DHS Information System Security Plan and Security Authorization Guide*, and supported by the automated Information Assurance Compliance System. Specific to PIV-enablement, the DHS Under Secretary for Management's July 22, 2015 memorandum requires components to implement PIV-based strong authentication for privileged and unprivileged access. Component Heads are required to submit Letters of Acceptance of Risk to the Under Secretary for Management for noncompliance and detailed corrective action plans for achieving compliance. The DHS CISO reviews the letters and plans.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

The DHS OCIO's ICAM office also established a process for querying and reporting on components' PIV implementation status each month. For components not in compliance, the DHS Deputy Under Secretary for Management, Chief Financial Officer, CIO, and CISO meet quarterly with each component's Deputy Head, CFO, CIO, and CISO to discuss status and agree on remediation actions to achieve compliance. While past meetings have resulted in significant progress in PIV-enablement, the goal of 100 percent has not yet been achieved due to significant system and/or resource limitations. Components are required to accept the risk through the risk management process as corrective actions continue. The DHS Deputy Under Secretary for Management's meetings with the components continue to focus on compliance gaps. Additionally, the DHS CISO generates a monthly scorecard on the status of a variety of cybersecurity metrics, including PIV implementation. The scorecard is issued to DHS and component leadership monthly, reminding that they are accountable for PIV-enabling all unclassified information systems under their purview. Management requested that OIG consider this recommendation open and resolved pending completion of the aforementioned activities, estimated for September 30, 2018.

OIG Analysis

We believe that the described actions satisfy the intent of this recommendation. This recommendation will remain open and resolved until the Department provides documentation to support that the planned corrective actions are completed.

Recommendation 7: Develop and implement a process requiring verification and validation of all component reporting to OCSO on their activities to meet HSPD-12 requirements.

Management Response

Concur. The DHS OCIO and DHS OCSO will use DHS implementation of Continuous Diagnostics and Mitigation Phase II initiative to provide "near real-time" validated reports of identification of a user's strong authentication security posture. The DHS OCIO and DHS OCSO will also continue to leverage the ICAM Executive Steering Committee as a key resource to help inform additional development and implementation of a verification and validation process, as required. Further, the DHS OCIO and DHS OCSO will take steps to validate that all PIV cards are issued pursuant to FIPS 201, as confirmed via independent assessments. Management requests that OIG consider this recommendation open and resolved pending completion of these activities, estimated for November 30, 2018.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

OIG Analysis

We believe that the described actions satisfy the intent of this recommendation. This recommendation will remain open and resolved until the Department provides documentation to support that the planned corrective actions are completed, including implementing a process requiring verification and validation of all component reporting to OCSO on HSPD-12 compliance activities.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Appendix A

Objective, Scope, and Methodology

The DHS Office of Inspector General (OIG) was established by the *Homeland Security Act of 2002* (Public Law 107-296) by amendment to the *Inspector General Act of 1978*. This is one of a series of audit, inspection, and special reports prepared as part of our oversight responsibilities to promote economy, efficiency, and effectiveness within the Department.

Our objective was to assess DHS' progress in implementing and managing the HSPD-12 program since prior audits in 2007 and 2010. Our audit focused on the requirements outlined in —

- HSPD-12, *Policy for a Common Identification Standard for Federal Employees and Contractors*;
- OMB M-05-24, *Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors*; and
- FIPS 201, *Personal Identity Verification (PIV) of Federal Employees and Contractors*.

In addition, we reviewed Federal laws and agency guidance, policies, and procedures related to HSPD-12 requirements.

We performed fieldwork at DHS headquarters and component organizations in the Washington, DC area. We researched background information, including laws, regulations, guidance, and prior audit reports related to HSPD-12 implementation. Within the OCSO, we interviewed Physical Security Division officials and representatives of ESSD responsible for HSPD-12 program management, including PIV card issuance and PACS implementation. Within the Office of the CIO, we interviewed the Acting CISO, as well as representatives of Enterprise IT Services and FISMA Compliance and Metrics to discuss technical support for instituting LACS.

Further, we reached out to officials within the Office of the Chief Human Capital Officer and the Office of the Chief Procurement Officer to learn about how DHS tracked employees and contractors onboard. We also held meetings with security officers and other representatives of FEMA, ICE, CBP, FLETC, Secret Service, TSA, USCIS, Coast Guard, and FPS officials within National Protection and Programs Directorate told us about their role in securing DHS facilities. From across these locations,



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

we obtained and analyzed supporting documentation to determine progress and identify challenges in meeting HSPD-12 requirements.

We conducted this audit between June 2016 and August 2017 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.

We appreciate DHS management efforts to provide the necessary information and access to accomplish this audit. Appendix E contains major contributors to this report.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Appendix B
Management Comments to the Draft Report

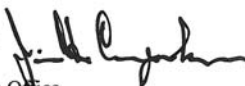
U.S. Department of Homeland Security
Washington, DC 20528



**Homeland
Security**

January 24, 2018

MEMORANDUM FOR: Sondra F. McCauley
Assistant Inspector General
Information Technology Audits

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

SUBJECT: Management's Response to OIG Draft Report: "Department-wide
Management of HSPD-12 Program Needs Improvement"
(Project No. 16-070-ITA-DHS, ICE, FLETC, NPPD)

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

DHS remains committed to ensuring enhanced and effective oversight capabilities are employed to meet Homeland Security Presidential Directive (HSPD) 12 requirements for identity credentials issued to federal employees and contractors requiring access to federally controlled facilities and information systems. DHS programs and efforts related to Cyber Security, Identity Management, and Physical and Logical Access Control depend on the full-scale issuance of DHS Personal Identity Verification (PIV) Cards to Department employees and contractors. The Department has effectively implemented mandatory logical access for more than 99 percent of all DHS employees and contractors accessing the network, to include having email addresses on the card in order to facilitate logical access requirements.

The Department has also deployed 630 Enrollment/Issuance Workstations and more than 40,000 Light Activation Stations in an estimated 1,079 DHS facilities/sites, 445 PIV Card Issuance Facilities (PCIF) across the United States, and 14 overseas locations in support of functions required to produce, issue, and maintain PIV cards or derived PIV credentials. The HSPD-12 Program is effectively coordinating efforts to increase efficiency, maintain standards, exceed expectations, and establish consistency, security, and sound oversight.

It is also important to highlight that in order to attain the security and interoperability goals of HSPD-12, the Identity Management System (IDMS) and PIV card application were successfully updated to ensure operational readiness and integrated into the Department to support the following:



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

- Derived PIV credentials for mobile information technology devices that enhance the security of information, which conforms to and satisfies the requirements of Federal Information Processing Standards (FIPS) 201-2 and related documents;
- System interconnections with physical and logical access systems, which include Physical Access Control Systems (PACS) of Federal Emergency Management Agency (FEMA), DHS Headquarters (HQ), U.S. Immigration and Customs Enforcement, Federal Law Enforcement Training Centers (FLETC), and the DHS Trusted Identity Exchange that support secure connections with internal and authoritative DHS systems;
- The HSPD-12 Testing and Evaluation Lab, which supports operational and user testing of DHS IDMS infrastructure to include system-to-system integration testing, credential functionality, security testing, interface testing, multiple modality (fingerprint, iris, facial) testing, PACS infrastructure and interoperability testing, and a Test as a Service for proof of concept demonstrations and user acceptance testing;
- Integration with 1) Automated Biometric Identification System (IDENT) to streamline the background investigation and fingerprint capture process, reduce duplicative infrastructure, establish a technical chain of trust, and provide continuous vetting; 2) U.S. Treasury's Public Key Infrastructure (PKI) to facilitate PIV card and credential issuance and management; and 3) DHS infrastructure, networks, monitoring, configuration and patch management solutions, and Data Centers;
- Tracking and management of all biometric, biographic, card, certificate, and credential attributes during the operational and audit lifecycle of an individual's identity with the capability of aggregating data from authoritative and non-authoritative data sources as well as correlating, searching, linking, and de-conflicting personnel identity data; and
- An authentication mechanism used to validate Pocket Credentials and increase security by validating credential recipients' identities within IDMS - efforts that seek to reduce costs incurred by issuing credentials through multiple disparate applications and databases.

Although PACS used throughout DHS are not yet fully compliant with HSPD-12, FEMA has effectively implemented a PACS system and commensurate controls for managing facility security risks in such a way that is fully compliant. FEMA's approach was established by inventorying and assessing each facility to determine the Facility Security Level, and through thorough implementation of an enterprise PACS product that leverages card readers that accept PIV cards. FEMA continuously monitors the DHS IDMS for changes in PIV cardholder information, allowing immediate changes and revocation of access privileges for separated employees and contractors.

The draft report contained seven recommendations, with which DHS concurs. Attached find our detailed response to each recommendation. Technical comments were previously provided under a separate cover.

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.

Attachment



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Attachment: Management Response to Recommendations Contained in 16-070-ITA-DHS, ICE, FLETC, NPPD

The OIG recommended that the DHS Chief Security Officer:

Recommendation 1: Develop and implement a process to collect, revoke, deactivate, and destroy the PIV cards of all contractors that no longer require access to DHS facilities or systems.

Response: Concur. It should be noted that DHS OCSO staff brought this requirement to the OIG's attention as it is a known challenge for which the HSPD-12 Program already has a mitigation plan in place. Successfully implementing this recommendation requires a mechanism to track, manage, and inform the HSPD-12 Program when a contractor is off boarding. The DHS PIV Card Issuer Operations Plan exists today to provide the process for collecting, deactivating, and destroying PIV cards of all contractors and we are working to improve our monitoring of these processes. In addition, DHS OCSO staff continue to work with the DHS Office of the Chief Information Officer (OCIO) Access Lifecycle Management (ALM) Project Team to address this recommendation. Specifically, ALM is being implemented to manage the lifecycle of access for employees and contractors at DHS, which will improve the Department's ability to identify active contractors by providing the ability to:

1. Identify who is on a contract at any time,
2. Off board a contractor at any time,
3. Off board contractors based on contract expiration, and
4. Certify quarterly that contractors on task orders are still required.

Each of these processes can result in off boarding from DHS to include removal of logical (information technology) access, physical access, a notification to the federal point of contact to collect the PIV card, and an automated inactivation of the PIV card. The ALM pilot at DHS Headquarters should be completed by March 31, 2018, and it will be expanded to the Management Directorate in the fourth quarter of FY 2018. At that point, ALM will provide an enterprise service to Components, to help address this same challenge.

We request that OIG consider this recommendation open and resolved pending completion of the aforementioned activities. Estimated Completion Date (ECD): September 30, 2018.

Recommendation 2: Develop and implement a plan that removes facility and information system access for all PIV cards after their credentials are revoked.

Response: Concur. DHS has established a project to automate the provisioning and de-provisioning of system and facility access through the ALM solution. ALM integrates with DHS information technology and establishes capabilities to remove system and facility access when the corresponding PIV card is revoked. OCSO and OCIO will continue the deployment of ALM and revise plans accordingly until integration with Logical Access Control Systems (LACS) and



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

PACS is complete. OCSO, in cooperation with OCIO, will also work with DHS Components to establish corresponding policies and procedures, as needed.

We request that OIG consider this recommendation open and resolved pending completion of the aforementioned activities. ECD: September 30, 2018.

Recommendation 3: Develop and implement a plan for providing sufficient guidance, funding, staffing, and oversight for procuring and implementing PACS Department-wide.

Response: Concur. In order to address the development and implementation of the PACS Modernization Strategy, OCSO will author and implement a plan for providing sufficient guidance, funding, staffing, and oversight for procuring and implementing PACS department-wide. The majority of PACS assets operated within the Department at the current time do not fully support our ability to implement the use of PIV and PKI. Most assets will require some form of hardware and software upgrades or replacement as a result. The activities needed to address these issues are already underway through the current DHS PACS Modernization effort. An Integrated Project Team (IPT) has been convened to look at challenges and/or constraints that may be encountered during the implementation of PACS Modernization. The IPT assessed current capability, generating the findings as a gap analysis. The gap analysis will be used to develop a Capability Assessment Report (per the DHS Joint Requirements Council process), to include a series of recommendations ranging from non-material change requests in the form of physical access control policy updates, audit/oversight functions, cost estimation capability, and options to be considered by DHS senior leadership to achieve full Federal Identity, Credential, and Access Management (FICAM) compliance.

We request that OIG consider this recommendation open and resolved pending completion of the aforementioned activities. ECD: September 30, 2018.

Recommendation 4: Implement a plan that confirms that DHS components inventory their facilities, identify facility security levels, pinpoint existing mechanisms for securing facilities, and quarterly report to the OCSO on progress made, to assist in accurately estimating the requirements and costs of PACS implementation.

Response: Concur. A PACS Reporting Tool has already been developed, and a pilot release with DHS HQ, FEMA, and FLETC began on January 8, 2018 and will be expanded to the other Components in the third quarter of FY 2018. This tool was developed to identify all DHS-occupied facilities, the associated facility security level designations, and detailed information on currently used PACS assets. The information received will be used to support OCSO/OCIO tracking of PACS, their authorization to operate, and use of approved products as reflected by the GSA-Approved Products List used in the quarterly FICAM reporting. Additionally, the catalogued information will be used to monitor Component progress in achieving PACS Modernization. The reporting tool is being coordinated with the DHS Office of the Chief Readiness Support Officer to build upon known facility information. Data analytics will be developed by OCSO and used with the facility data received as a means of planning physical access control systems implementation requirements and cost estimates.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

We request that OIG consider this recommendation open and resolved pending completion of the aforementioned activities. ECD: September 30, 2018.

Recommendation 5: Coordinate with the Chief Information Officer on ensuring that components conduct valid and current risk assessments for information systems under their purview as a means of identifying requirements for logical access control systems implementation.

Response: Concur. The DHS OCSO and DHS OCIO will coordinate HSPD-12 implementation as it pertains to risk assessments for information systems. The DHS OCIO's Office of the Chief Information Security Officer (OCISO) has had policies, procedures, and a process in place preceding, during, and subsequent to this audit to hold Components accountable for conducting risk assessments for the unclassified information systems under their purview. For example, the DHS OCISO requires through the *DHS Sensitive Systems Policy Directive 4300A* that risk assessments be conducted as part of the assessment and authorization process. The systems authorization process is implemented through the required use of the DHS automated Information Assurance Compliance System (IACS). This system holds Components accountable for conducting the risk assessment by: 1) Not allowing Components to progress through the authorization steps until the risk assessment is completed, and 2) Requiring the Component CISO or equivalent to confirm that the risk assessment is valid, complete, and current. The tool uses the results of the assessment to generate the required security controls baseline, which includes the IACS, to be implemented by the Component system. Risk assessments for Component systems are also required to be updated or revised when the system authorization to operate is refreshed or according to other policy requirements for specialized systems. Component CISOs are also permitted by the National Institute of Standards and Technology and DHS policy to tailor controls based on their environments and mission requirements.

We request that OIG consider this recommendation resolved and closed.

Recommendation 6: Coordinate with the Chief Information Officer on ensuring that components PIV-enable all unclassified information systems under their purview.

Response: Concur. The DHS OCSO and DHS OCIO will coordinate HSPD-12 implementation as it pertains to PIV-enablement of all unclassified information systems. The DHS OCIO has had a process in place to hold Components accountable for PIV-enabling unclassified information systems for which the Component is responsible. The *DHS Sensitive Systems Policy Directive 4300A* (Policy ID statements 3.14.7.f - 3.14.7.i) requires the use of PIV credentials to access existing and new systems. The 4300A policy was changed pursuant to the issuance of the DHS Under Secretary of Management's memorandum, *Strengthening DHS Cyber Defenses*, dated July 22, 2015. The 4300A policy also states that system owners are responsible for the successful operation of the information systems and programs within their program area and are ultimately accountable for their security. The system owner ensures information security compliance, development, and maintenance of security plans, user security training, notifying officials of the need for security authorization, and need to resource (Policy ID statement 2.2.9.d).



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

The DHS OCIO uses its risk management process to hold the Components accountable for PIV-enabling its unclassified information systems. The process is required by the 4300A policy, defined in the *DHS Information System Security Plan and Security Authorization Guide*, and supported by the automated Information Assurance Compliance System. Specific to PIV-enabling, the DHS Under Secretary for Management issued a memorandum, *Strengthening DHS Cyber Defenses*, dated July 22, 2015, requiring Components to implement PIV-based strong authentication for privileged and unprivileged access. Component Heads are required to submit Letters of Acceptance of Risk to the Under Secretary for Management for non-compliance and detailed corrective action plans for achieving compliance. The DHS Chief Information Security Officer (CISO) reviews the letters and plans received by the non-compliant Components. The DHS OCIO ICAM office also established a process of querying and reporting on Components PIV implementation status each month. For the Components not in compliance, the DHS Deputy Under Secretary for Management, Chief Financial Officer (CFO), CIO, and CISO meet quarterly with each Component's Deputy Head, CFO, CIO, and CISO to discuss status and agree on remediation actions to achieve compliance. While past meetings have resulted in significant progress in PIV enablement, the goal of 100 percent has not yet been achieved due to significant system and/or resource limitations. Components are required to accept the risk through the risk management process as corrective actions continue. The DHS Deputy Under Secretary for Management meetings with the Components continue to focus on the compliance gaps.

Additionally, the DHS CISO generates a monthly scorecard on the status of a variety of cybersecurity metrics, which includes PIV implementation. The scorecard is issued to DHS and Component leadership monthly reminding leadership that they are being held accountable for PIV-enabling all unclassified information systems under their purview.

We request that OIG consider this recommendation open and resolved pending completion of the aforementioned activities. ECD: September 30, 2018.

Recommendation 7: Develop and implement a process requiring verification and validation of all component reporting to OCSO on their activities to meet HSPD-12 requirements.

Response: Concur. DHS OCIO and DHS OCSO will use the DHS implementation of Continuous Diagnostics and Mitigation Phase II initiative to provide "near real-time" validated reports of identification of a user's strong authentication security posture. DHS OCIO and DHS OCSO will continue to leverage the Identity, Credential, and Access Management Executive Steering Committee as a key resource to help inform additional development and implementation of a verification and validation process as required. Further, DHS OCIO and DHS OCSO will take steps to validate that all PIV cards are issued pursuant to FIPS 201 as confirmed via independent assessments.

We request that OIG consider this recommendation open and resolved pending completion of the aforementioned activities. ECD: November 30, 2018.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Appendix C
Major HSPD-12 Milestones and Requirements

Originator	Date	Initiative or Action	Purpose
Office of the President of the United States	August 2004	Homeland Security Presidential Directive (HSPD) 12 signed and issued	Established a policy for creation, issuance, and use of personal identification credentials in the Federal Government and required the development and use of a standard for secure and reliable forms of identification for Federal employees and contractors.
Dept. of Commerce National Institute of Standards and Technology (NIST)	February 2005	Federal Information Processing Standards (FIPS) 201, <i>Personal Identity Verification (PIV) of Employees and Contractor Employees</i> , was released	Established standards for secure and reliable forms of identification credentials, background checks of government employees and contractors, and identification cards used for entering government facilities and for accessing information systems.
Office of Management and Budget (OMB)	August 2005	Memorandum 05-24 (M-05-24) - <i>Policy for a Common Identification Standard for Federal Employees and Contractor Employees</i>	Outlined guidance and deadlines for Federal departments and agencies to follow when implementing HSPD-12.
OMB	February 2006	Memorandum 06-06, <i>Sample Privacy Documents for Agency Implementation of Homeland Security Presidential Directive (HSPD) 12</i>	Provided executive Departments and agencies sample privacy documents to use as models in implementing HSPD-12 privacy requirements.
DHS Office of Chief Security Officer (OCSO)	March 2006	Established the first HSPD-12 Program Management Office (PMO) within DHS.	In response to the requirement to establish a PMO to oversee and guide headquarters and component HSPD-12 efforts across DHS.
OMB	June 2006	Memorandum, M-06-18, <i>Acquisition of Products and Services for Implementation of HSPD-12</i>	To establish a set list of General Services Administration approved items and vendors for the acquisition of HSPD-12 products and services.



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

HSPD-12 Milestones and Requirements, continued

Originator	Date	Initiative or Action	Purpose
OCSO	October 2006	Memorandum, <i>HSPD-12 Requirements for All DHS Personnel</i>	Provided requirements for all DHS components must adhere to the FIPS 201 minimum requirements as well guidance outlined in an attachment. Made specific suitability standards and entrance-on-duty procedures beyond those requirements the prerogative of the component to comply.
Office of Personnel Management	July 2008	Memorandum, <i>Final Credentialing Standards for Issuing Personal Identity Verification (PIV) cards under HSPD-12</i>	Provided government-wide credentialing standards to be used by all Federal departments and agencies in determining whether to issue or revoke personal identity verification (PIV) cards to their employees and contractor personnel, including those who are non-United States citizens.
OMB	February 2011	OMB 11-11, <i>Continued Implementation of Homeland Security Presidential Directive (HSPD) 12- Policy for a Common Identification Standard for Federal Employees and Contractor Employees</i>	Directed each agency to develop and issue policy by March 31, 2011, requiring the use of the PIV credentials as the common means of authentication for access to that agency's facilities, networks, and information systems.
DHS Office of Management	July 2012	Memorandum, <i>Implementation of Mandatory Use of the Personal Identity Verification (PIV) Card to Access DHS Networks</i>	To enhance security by requiring PIV cards to access unclassified networks. The goal was 50 percent compliance by fiscal year 2013 and 75 percent compliance by fiscal year 2014 across all DHS components.
OMB	November 2013	<i>Fiscal Year 2013 Reporting Instructions for the Federal Information Security Modernization Act and Agency Privacy Management</i>	Identified HSPD-12 PIV card use with strong authentication a priority across the Federal Government. Additionally, (1) all information technology system applications reported as part of <i>Federal Information Security Modernization Act</i> would use the PIV credential as the means to gain access, and (2) physical access control systems are included in the count of reported systems.

Source: OIG-developed



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Appendix D

Detailed Description of PIV Subsystems

Subsystem 1: PIV Card Issuance and Management

Per FIPS 201, the identity proofing and registration component (illustrated in subsystem 1, PIV Card Issuance and Management, of figure 2) refers to the process of collecting, storing, and maintaining all information and documentation that is required for verifying and assuring a card applicant's identity. This process deals with the personalization of the physical (e.g., visual exterior) and logical (ICC content) aspects of the card at the time of issuance and includes maintenance thereafter. The process includes printing photographs, obtaining names and other information on the card, and loading the relevant card certificates, biometrics, and other data. The key management process is responsible for generation of key pairs, issuance and distribution of digital certificates containing the public keys of the cardholder, and management and dissemination of certificate status information. Key management is used throughout the lifecycle of PIV cards — from generation and loading of authentication keys and PKI credentials, to use of the keys for secure operations, to eventual key reissuance or termination of the card. It is also used to update any change in cardholder status (e.g., termination). To be issued a PIV card, each applicant must have —

- successfully met minimum security requirements, including a favorable suitability check;
- favorably completed a National Agency Check with Inquiries, or equivalent; and
- successfully passed adjudication via the Federal Bureau of Investigations' National Criminal History Check (fingerprint check).

Within the PIV System, enrolling officials compile and track an applicant's personal suitability and security clearance using the Integrated Security Management System. These security processes are automated in order to provide information for the adjudicator to render a decision on the status of an applicant. Once favorable suitability is determined, an enrolling official initiates a request to issue the applicant a PIV card. If confirmed, the applicant's personal data is electronically transferred from the ISMS to the IDMS, which facilitates identity proofing, PIV card issuance and maintenance, and key management. These three processes are depicted in the upper left portion of figure 2.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Shortly after entrance-on-duty, an applicant is required to report to a PCIF. When the applicant arrives at the PCIF, the PIV card registration process is initiated. The first step in this process consists of *identity proofing*, during which the applicant must provide two forms (one primary and one secondary) of identity source documents in original form.²⁶

The primary identity source document shall be one of the following forms of identification:

- U.S. Passport or a U.S. Passport Card;
- Permanent Resident Card or an Alien Registration Receipt Card (Form I-551);
- Foreign passport;
- Employment Authorization Document containing a photograph (Form I-766);
- Driver's license or identification (ID) card issued by a state or territory of the United States, provided it contains a photograph;
- U.S. Military ID card;
- U.S. Military dependent's ID card; or
- Previously issued PIV card.

The secondary identity source document may be from the preceding list, but cannot be of the same type as the primary identity source document.²⁷ A secondary identity source document may also be one of the following:

- U.S. Social Security Card issued by the Social Security Administration;
- An original or certified copy of a birth certificate issued by a state, county, municipal authority, or territory of the United States bearing an official seal;
- ID card issued by a Federal, state, or local government agency or entity, provided it contains a photograph;
- Voter's registration card;
- United States Coast Guard Merchant Mariner Card;
- Certificate of U.S. Citizenship (Form N-560 or N-561);

²⁶ FIPS 201, *Personal Identity Verification of Federal Employees and Contractors*, August 2013, stated that departments and agencies may choose to accept only a subset of the identity source documents listed in this section.

²⁷ For example, if the primary source document is a passport, the secondary source document should not be another (i.e., foreign) passport.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

- Certificate of Naturalization (Form N-550 or N-570); or
- U.S. Citizen ID Card (Form I-197).

Both forms of identification are collected from the applicant and compared to the applicant's information contained in IDMS. This comparison authenticates the applicant's identity and also creates a "chain of trust" record for these documents. Once this process is complete, the *enrollment process* begins. During this process, IDMS peripheral equipment (e.g., cameras and biometric scanners) is used to collect facial images and biometric data from the applicant, which becomes part of the applicant's enrollment record. After this is completed, the PIV card issuance and key management processes are initiated.

An enrollment official prints the PIV card, downloads certificates to the card's integrated circuit chip (ICC), and activates the PIV card in IDMS. Once activated, the downloaded certificates determine the applicant's physical and logical access. These certificates are also programmed at the cardholder's respective security office. The enrollment official next downloads the PKI certificates (from IDMS) to the card's ICC and instructs the applicant to enter a PIN that is not easily guessable. This PIN is used during the cardholder authentication process when required to access a controlled physical or logical asset. The enrollment official then tests the PIV card to ensure it is activated in IDMS. Finally, the enrollment official compares the applicant's fingerprints against biometric data stored within the applicant's PIV enrollment record in IDMS. Upon identity confirmation, the applicant is issued a PIV card.

After the PIV card is issued to the applicant, the PIV System Issuance and Management Subsystem maintains information stored on the PIV card until PIV card termination, once the card is no longer needed. According to FIPS 201, the data and credentials stored on a PIV card may need to be updated or invalidated prior to the card expiration date if —

- the cardholder changes his or her name;
- the cardholder retires, or changes jobs; or
- the cardholder's employment is terminated, thus requiring invalidation of the card.

Subsystem 2: Physical and Logical Access Points

Per FIPS 201, physical and logical access points (figure 2, subsystem 2) are where a cardholder uses a PIV card to access physical and logical resources. This subsystem typically consists of either (1) a PIV card reader, (2) a card reader with a PIN input device, or (3) a biometric card reader. Note that some



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

access points only require visual inspection of the PIV card by an authorized official (e.g., security guard) for physical access.

When the cardholder presents a PIV card at an access point, the card reader communicates with the PIV card to retrieve the cardholder's authorization information from card's ICC. The card reader then relays that information to the access control system (figure 2, subsystem 3) where access is desired. At this point, access control is turned over to subsystem 3 for cardholder authentication and determination of authorization.

Subsystem 3: Cardholder Authentication and Authorization

The third subsystem in the PIV system involves authenticating the cardholder and verifying authorization to enter a controlled facility or access an information system. Per FIPS 201, this cardholder authentication and authorization subsystem depicted in figure 2 involves physical and logical access control systems, protected (facility and information systems) assets, and the authorization data used to allow cardholder access.

Each time a cardholder's authentication data is passed from a PIV card to the physical or logical resource the cardholder desires to access, that information is compared to authentication data stored in the particular physical or logical access control system. Once the cardholder's identity is authenticated, the PIV system queries the cardholder's access permissions it stores and grants access accordingly.



OFFICE OF INSPECTOR GENERAL

Department of Homeland Security

Appendix E

Office of IT Audits Major Contributors to This Report

Richard Saunders, Director, Advanced Technology Projects
Alexander Granado, Audit Manager
Daniel McGrath, Program Analyst
Frederick Shappee, Referencer



OFFICE OF INSPECTOR GENERAL
Department of Homeland Security

Appendix F
Report Distribution

Department of Homeland Security

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