Department of Homeland Security
Office of Inspector General

Resource and Security Issues Hinder DHS' Implementation of Homeland Security Presidential Directive 12

OIG-10-40

January 2010

Office of Inspector General

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

Homeland
Security

January 25, 2010

Preface

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

This report addresses the strengths and weaknesses of DHS' program and security management of its implementation of Homeland Security Presidential Directive 12 requirements. It is based on interviews with selected employees, contractor personnel, and management officials, including the Chief Security Officer; direct observations; system security vulnerability assessments; and a review of applicable documents.

The recommendations herein have been developed to the best knowledge available to our office, and have been discussed in draft with those responsible for implementation. We trust this report will result in more effective, efficient, and economical operations. We express our appreciation to all of those who contributed to the preparation of this report.

Richard L. Skinner

Richard L. Skinner
Inspector General

Table of Contents/Abbreviations

Appendices

Abbreviations

ACO	Access Control Office
ATO	Authority to Operate
C&A	certification and accreditation
CA	Certificate Authority
CBP	Customs and Border Protection
DHS	Department of Homeland Security
EIWS	enrollment and issuance workstations
FEMA	Federal Emergency Management Agency
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FLETC	Federal Law Enforcement Training Center
FTE	full-time equivalent
FY	Fiscal Year
GFE	government furnished equipment
GSA	General Services Administration
HSPD-12	Homeland Security Presidential Directive 12

ICE	Immigration and Customs Enforcement
ICISS	Identification and Credential Issuing Station and System
IDMS	Identity Management System
ISSO	Information Systems Security Officer
IT	information technology
ITSO	Information Technology Services Office
NAC	Nebraska Avenue Complex
NIST SP	National Institute of Standards and Technology Special Publication
NPPD	National Protection and Programs Directorate
OCIO	Office of Chief Information Officer
OCSO	Office of the Chief Security Officer
OMB	Office of Management and Budget
PACS	Physical Access Control System
PII	personally identifiable information
PIN	personal identification number
PIV	Personal Identity Verification
PKI	Public Key Interface
PMO	Program Management Office
SBCG	Secure Baseline Configuration Guide
SELinux	Security Enhanced Linux
SSO	Special Security Officer
SU	super user
TAF	Trusted Agent FISMA
TS/SCI	Top Secret/Sensitive Compartmented Information
TSA	Transportation Security Administration
USCIS	United States Citizenship and Immigration Services

Executive Summary

Homeland Security Presidential Directive 12 (HSPD-12), *Policy for a Common Identification Standard for Federal Employees and Contractor*s, requires the development and agency implementation of a mandatory, government-wide standard for secure and reliable forms of identification for federal employees and contractors. All federal departments and agencies are to implement an HSPD-12 program to meet the standard established by the policy, which aims to enhance security, increase government efficiency, reduce identity fraud, and protect personal privacy.

An accurate determination of identity is essential to make sound decisions when granting an individual access to security-sensitive government buildings and other facilities, computer systems, or data. Successful implementation of the directive's requirements will strengthen access controls, increase the security of federal facilities and information systems, and reduce the potential for terrorist attacks.

Although DHS has established an identification credentialing and issuance process, the department has not made the implementation of an effective HSPD-12 program a priority. The original completion date for the issuance and use of identity credentials by all federal employees and contractors was October 27, 2008. As of September 22, 2009, only 15,567, of the approximately 250,000 department employees and contractors, had been issued identity credentials.

Due to weak program management, including insufficient funding and resources, and a change in its implementation strategy, the department is well behind the deadline for fully implementing an effective HSPD-12 program. In addition, the department faces significant challenges in meeting HSPD-12 directive requirements for logical access to its information systems. Furthermore, system security and account management controls are not effective in protecting personally identifiable information collected and stored from unauthorized access. Existing security issues must be addressed to allow for the deployment of a robust, efficient, and secure interoperable identity card and issuance system department-wide.

We are making 15 recommendations to DHS' Chief Security Officer, in conjunction with the Chief Information Officer. DHS management

concurred with the recommendations and has already begun to take the actions to implement them. The resolved recommendations will remain open until DHS provides documentation to support that the implementation of all planned corrective actions is complete. DHS' response is summarized and evaluated in the body of this report and included, in its entirety, as Appendix B

Background

Traditionally, a wide range of mechanisms has been employed to authenticate an individual's identity, using various classes of credentials for both physical access to buildings and authorization to access computers and data. HSPD-12 established the policy for a common standard for identification credentials issued by government departments and agencies to its employees and contractors. These credentials are to be used for gaining physical access to federally controlled facilities and logical access to federally controlled information systems.

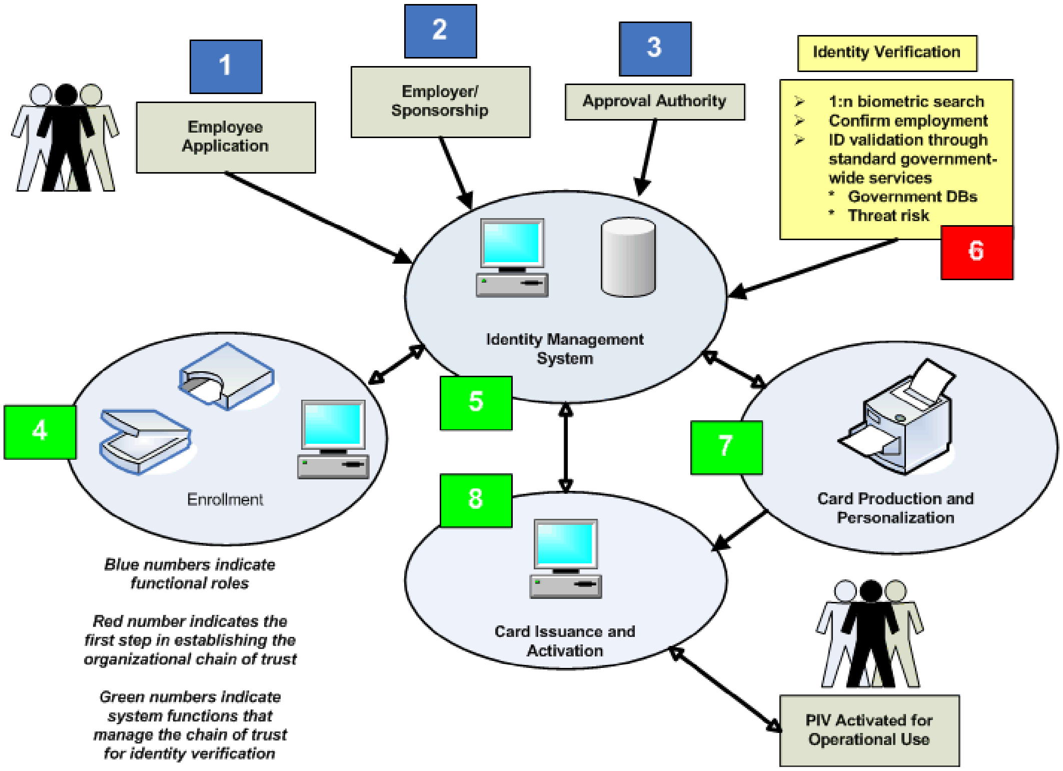
The Department of Commerce was tasked with developing the standard that specifies the architecture and technical requirements for a common identification standard for federal employees and contractors. The government-wide standard for secure and reliable forms of identification credentials is defined in the Department of Commerce' Federal Information Processing Standards (FIPS) publication 201-1, *Personal Identity Verification (PIV) of Federal Employees and Contractors*. Figure 1 illustrates the minimum mandatory components and roles required to support PIV control objectives and requirements according to FIPS 201-1.

To support the implementation of HSPD-12, the Office of Management and Budget (OMB) issued Memorandum 05-24 (M-05-24), *Implementation of Homeland Security Presidential Directive (HSPD) 12 - Policy for a Common Identification Standard for Federal Employees and Contractors*. This memorandum outlined the instructions and guidance, as well as deadlines, for federal departments and agencies to follow when implementing HSPD-12. According to the OMB memorandum, agencies were required to complete the background investigations on all current employees and contractors and to issue identity credentials according to the following schedule:

- October 27, 2007 - Agencies were to complete background checks and issue credentials to all employees and contractors with 15 or fewer years of service.
- October 27, 2008 - Agencies were to complete background checks and issue credentials to all employees with more than 15 years of service.

Additionally, departments and agencies were to identify federally controlled facilities, information systems, and other federal applications that were important for security.

Figure 1: PIV Identity Verification and Issuance


1
Employee Application
2
Employer/ Sponsorship
3
Approval Authority
Identity Verification
1:n biometric search
Confirm employment
ID validation through standard government-wide services
* Government DBs
* Threat risk
6
Identity Management System
4
Enrollment
5
7
Card Production and Personalization
8
Card Issuance and Activation
PIV Activated for Operational Use
Blue numbers indicate functional roles
Red number indicates the first step in establishing the organizational chain of trust
Green numbers indicate system functions that manage the chain of trust for identity verification

In October 2007, we reported that the department was experiencing delays in developing a technical solution capable of issuing PIV cards to its employees and contractors.[1] Subsequently, OMB granted DHS an extension, until December 2010, to issue PIV cards to its workforce.

We also reported that DHS had neither assessed the total cost to implement HSPD-12 department-wide nor identified the extent to which PIV cards would be used or required to access facilities and information systems. In addition, component implementation guidance needed to be updated, PIV card issuance statistics were not being posted to DHS’ public website, and the department had not yet identified a technical solution to issue PIV cards to its employees and contractors.

Our recommendations targeted the identification of resources to carry out DHS’ implementation plan, development of a department-wide cost

[1] *Progress Has Been Made But More Work Remains in Meeting Homeland Security Presidential Directive 12 Requirements* (OIG-08-01), October 2007.

estimate, a decision on facility access points and information systems requiring the use of PIV cards, revisions to component guidance, certification and accreditation of the information systems used to implement HSPD-12 and FIPS 201-1, and the posting of PIV card statistics on the department's website. Our current audit was conducted to follow up on our prior audit recommendations and assess DHS' progress in meeting HSPD-12 implementation requirements.

Results of Audit

Actions Taken to Implement DHS' HSPD-12 Program

DHS' Office of Security is responsible for the department's HSPD-12 program, with technical support from the Office of the Chief Information Officer (OCIO). DHS is implementing HSPD-12 by issuing biometric smartcards, known as DHS PIV cards. DHS PIV cards will be issued to all DHS employees and contractors, an estimated 250,000 individuals.[2] DHS began issuing these cards to Headquarters employees and contractors in June 2008.[3] DHS uses two systems to support its PIV card issuance process and use. These systems are the Identity Management System (IDMS) and the Headquarters Physical Access Control System (PACS).[4] To support HSPD-12 and FIPS 201-1 requirements, the department has:

- Worked with stakeholders in the DHS components, through an HSPD-12 Council and working groups, to develop a coordinated departmental approach to implementation.

- Awarded a blanket purchase agreement for the component purchase of DHS PIV related technology, such as card enrollment and issuance workstations (EIWS).

- Conducted a pilot to test the use of PIV cards for logical access within the National Protection and Programs Directorate (NPPD). NPPD employees and contractors are continuing to use PIV cards to access DHS' information systems.

[2] The United States Coast Guard is exempt and will continue to use the Department of Defense Common Access Card, except for those personnel who routinely access DHS-controlled facilities that have migrated to DHS PIV cards.
[3] DHS Headquarters consists of the Offices of the Chief Financial Officer, Chief Privacy Officer, Domestic Nuclear Detection, Federal Law Enforcement Training Center (FLETC), General Counsel, Inspector General, Intelligence and Analysis, and Policy.
[4] An electronic interface to connect IDMS and Headquarters PACS has not been developed or installed.

- Achieved PIV Card Issuer accreditation for Headquarters from the General Services Administration (GSA). Through this accreditation, GSA approved the configuration of DHS' PIV card.[5]

- Established the Identity Management Division within the Office of Security in June 2009. The Program Management Office (PMO), introduced in March 2006, became part of the Identity Management Division.

- Deployed card EIWS at Customs and Border Protection (CBP), Federal Emergency Management Agency (FEMA), FLETC, Headquarters, Immigration and Customs Enforcement (ICE), Transportation Security Administration (TSA), and United States Customs and Immigration (USCIS) during Fiscal Year (FY) 2009. The number of cards produced and issued to component personnel, as of September 22, 2009, is shown in Figure 2.

Figure 2: DHS PIV Cards Issued by Component

Component	Cards Issued
CBP	9
FEMA	3,113
FLETC	35
DHS Headquarters	11,875
ICE	8
TSA	5
USCIS	522
Total	**15,567**[6]

Despite the progress made, DHS still faces further delays and significant program and system management challenges in implementing an effective HSPD-12 program. For example, according to program management, DHS will not be able to meet the December 2010 extension OMB granted to complete issuing PIV cards to its employees and contractors. DHS' milestone for completion of PIV card issuance to employees and contractors is now September 30, 2011, a date that is almost three years after the mandated October 27, 2008, deadline established by OMB.

[5] Based on OMB M-07-06, *Validating and Monitoring Agency Issuance of Personal Identity Verification Credentials*, agencies were required to submit the configuration of their standard credential to GSA for testing and approval.

[6] Not all of the cards issued have been "activated" in IDMS and PACS. Of the 15,567 cards issued, 12,892 had been activated. The numbers include cards and cards that have been revoked and test cards.

DHS does not have a plan to successfully implement a robust program to increase physical and logical access security within the department. The absence of an HSPD-12 program implementation plan, department-wide deployment strategy, and sufficient resources are hindering progress. Components currently have their own individual physical access control systems, which will need to be consolidated into DHS' Headquarters PACS some time in the future. More work remains to ensure that existing infrastructures are consolidated to support DHS' HSPD-12 program. In addition, an interface between the card issuance system, IDMS, and PACS is needed. Necessary facility upgrades need to be completed at component locations to ensure PIV cards are interoperable with DHS' physical and logical access control systems.

Inadequate Program Management and Resources Have Led to Delays in DHS' Implementation of HSPD-12

Implementation of a fully functional identity management system is a significant effort requiring the coordination of various staff and resources. Implementing a fully functional smartcard infrastructure requires more than printing and issuing cards. Buy-in and active participation of leadership is essential to the success of a credentialing program.

A program management approach is to be established for all projects commensurate with the size, complexity, and project requirements. Sponsors of such programs should have sufficient authority to own the execution of a project within the overall strategic program. Smartcard implementation is a complex program management task. According to the *Federal Identity Management Handbook*, HSPD-12 requires program managers to procure and implement smartcard technology. Each agency is expected to allocate funding and resources to support the implementation of HSPD-12.

In June 2009, the department changed its strategy on how DHS PIV cards would be issued, from a component-by-component based implementation to a centrally managed regional strategy. Since this change in the department's implementation strategy, the PMO has not received adequate staffing or funding, developed a viable implementation and regional deployment plan, estimated the department-wide cost for implementing HSPD-12, or identified performance measures to properly track implementation progress. As a result, the department's full implementation of HSPD-12 has been effectively delayed until September 30, 2011.

DHS' PMO Was Not Adequately Staffed or Funded

DHS' PMO is responsible for implementing HSPD-12. Department leadership, however, did not provide adequate support, funding, or resources for the PMO to effectively manage and oversee DHS' implementation its HSPD-12 program. As a result, DHS is well behind schedule.

The PMO, established in March 2006, was initially staffed on an ad-hoc basis, and Security Office funding was often diverted to higher priority programs, such as security background investigations. Prior to October 2009, the PMO was not authorized any full-time equivalent (FTE) employees or funding for contractor staff. In its FY 2010 budget request, the Office of Security asked the department for funding for PMO staffing, but no FTE employees were authorized. The Office of Security authorized six FTE employees for the PMO in FY 2010. Five employees are currently onboard, and the PMO is in the process of converting one contactor employee to an FTE.

According to DHS management officials, the department-wide implementation of HSPD-12 has not been a priority. Therefore, DHS has not yet implemented a robust, efficient, and interoperable identity credentialing program to increase both physical and logical information security.

A Regional Program Implementation and Deployment Plan Has Not Been Developed

The PMO has not developed an implementation and deployment plan based on the centrally managed regional implementation strategy that DHS has employed to address HSPD-12 requirements. Though the PMO has begun to develop a new program implementation plan, it is unknown when the plan will be ready. Also, as we reported in 2007, DHS has not yet identified to what extent PIV cards will be used or required to access specific facilities or information systems throughout the department.

DHS' HSPD-12 program implementation plan should define the scope of work and the roles and responsibilities of key personnel. The plan should also identify facilities and information systems that will be affected and outline the card functions DHS will enable to authorize access to resources. In addition, the plan should include milestones for critical tasks associated with the issuance of PIV cards, such as the deployment of the new regional enrollment centers Furthermore, the plan should specify locations, estimate the numbers of staff to be processed through each facility, and identify when each location will receive card EIWS.

OMB M-05-24 requires agencies to develop an implementation plan, which must be submitted to OMB for review and approval. As we reported in October 2007, the Office of Security originally submitted an implementation plan to OMB. The implementation plan developed was based on component-by-component based milestones for the department's compliance with HSPD-12 requirements to meet the December 2010 deadline approved by OMB. However, the original plan became obsolete when the department changed its HSPD-12 program implementation strategy in June 2009. Further, without an implementation or deployment plan, the PMO determined that the department will be unable to meet OMB's extended December 2010 date. The new deadline date established by the PMO is September 30, 2011, but OMB has not approved this date.

DHS Has Not Developed a Department-Wide Cost Estimate

In our October 2007 report, we recommended that DHS develop a department-wide cost estimate to ensure that sufficient resources were allotted to implement HSPD-12. Although DHS concurred with this recommendation, it has not developed a department-wide cost estimate that includes all costs related to its HSPD-12 implementation.

Federal agencies and components were to fund HSPD-12 implementation from existing resources. Because component level resources were limited, DHS changed its strategy, in part, to better oversee and manage the components' implementation of HSPD-12. Additionally, the change to a regional HSPD-12 implementation strategy was expected to cost the department less to implement than the original plan.

The ability to meet the milestones for card issuance depends on the availability of funding and resources to meet the initial anticipated needs. Existing funding and resource issues related to the department's implementation of HSPD-12 have contributed to significant delays in meeting milestone dates for card issuance and full implementation of its HSPD-12 program.

The PMO established the following milestones for initial card issuance for the estimated 250,000 DHS employees and contractors:

- FY 2009 – Complete issuance to 10,000 federal employees and contractors.[7]
- FY 2010 – Complete issuance to 135,000 federal employees and contractors.
- FY 2011 – Complete issuance to 105,000 federal employees and contractors.

The current $25 million budget for FY 2010 is based on the costs associated with issuing 135,000 PIV cards. The costs are broken down in detail as follows:

- **Initial Issuance and Support:** Card issuance workstation leasing, installation, and maintenance (for 192 workstations), surge labor support (consisting of 60 contractors), PMO support, training, software leasing and license fees (for up to 200 locations), and development of three interfaces to connect vetted databases.
- **Issuance Consumables:** PIV card stock, badge holders, lanyards, and printer consumables.
- **Annual Enterprise Back-End System Costs Required to Support Technical Solution:** Maintenance of IDMS and interface to Certificate Authority (CA), IDMS license fee and server hosting, Treasury CA and maintenance fee, Public Key Interface (PKI) support (consisting of four contractors), PKI certificates and maintenance (for 250,000 identities), Virtual Private Network support, maintenance of Headquarters and component interfaces (currently five interfaces), and logical access enterprise middleware.

The same cost breakdown based on the initial issuance of the remaining 105,000 cards was used in developing the FY 2011 budget estimate.

The PMO determined that it cost $177 per PIV card issued in FY 2009.[8] Working under the assumption that the cost per card issued would remain the same, the projected cost for card issuance in FY 2010 would be approximately $24 million ($177 × 135,000 cards). With a budget of $25 million, little funding would remain to cover other costs not considered part of card issuance in the FY 2010 budget. For example, the cost of establishing PIV card enrollment centers at DHS' component locations are not covered in the card costs. Enrollment centers will be needed in FY 2010 to issue PIV cards. The FY 2010 budget also does not cover the costs

[7] DHS surpassed this goal; a total of 15,652 cards were issued in FY 2009.
[8] The cost per card is based on the issuance of 15,652 PIV cards in FY 2009 (October 1, 2008, through September 30, 2009).

associated with the installation of card readers at component facilities, development of an interface to connect IDMS and Headquarters PACS, consolidation of components' physical access systems into PACS, or the maintenance of PACS.

Logical access costs are not covered in the $22 million FY 2011 budget estimate even though logical access capability is expected to be implemented in the first quarter of FY 2011. Additionally, the cost of work to ensure that existing component infrastructures are interoperable with Headquarters PACS is not included in the FY 2011 budget estimate.

DHS' department-wide cost estimates for FYs 2010 and 2011 are based on the costs associated with PIV card issuance, not the department-wide implementation of HSPD-12. Costs for infrastructure and system upgrades associated with interoperability issues have not been considered, and these issues may take many years to address.

HSPD-12 Performance Measures Have Not Been Established

Quantifiable performance measures have not been developed to provide an overview of how DHS will meet its anticipated September 30, 2011, HSPD-12 implementation deadline. Since DHS' HSPD-12 PMO has not yet revised its implementation or deployment plan milestones, it is unable to determine the overall progress the department has made in implementing HSPD-12.

Performance measurement indicates what a program is accomplishing and whether results are being achieved. In addition, it helps management by providing information on how resources and efforts should be allocated to ensure effectiveness. OMB requires each agency to prepare an annual performance plan covering each program activity included in the budget of the agency. A performance plan should include the following:

- Goals that define the level of performance to be achieved by a program activity.
- Goals that are objective, quantifiable, and measurable.
- Performance indicators to measure or assess the relevant output, service levels, and outcomes of each program activity.
- A basis for comparing actual program results with established performance goals.

The PMO has not completed its plan for department-wide implementation of HSPD-12. The implementation plan should include milestones and goals that are quantifiable and measurable. In addition, though the PMO has requested that components submit a status of their progress regarding facility upgrades, such as installing and replacing card readers, not all of the components are submitting these reports. The PMO does not have the authority to make the components submit implementation status reports; therefore, the PMO is unable to measure the components' overall status and readiness for HSPD-12 compliance.

Conclusion

DHS' ability to meet card issuance and regional deployment milestones depends on the availability of staffing and resources. Insufficient funding and resources have, in part, caused the department's current delays in implementing an effective HSPD-12 program within OMB's timelines. The PMO, brought under the newly established Identity Management Division in June 2009, could not adequately manage the timely implementation of HSPD-12 because it was not properly funded or staffed.

Poor planning and program management, a change in the department's implementation strategy, and insufficient funding and resources have led to significant delays in issuing PIV cards timely and meeting OMB's deadline for implementing an effective HSPD-12 program. The delayed issuance of DHS PIV cards has limited the department's ability to enhance and strengthen its overall physical access security process based on credentialing technology. In addition, the delays have affected other parts of the department's compliance with HSPD-12 and FIPS 201-1, including logical access, and will affect DHS employee and contractor access to other federal buildings. Once implemented, a secure and interoperable HSPD-12 compliant card will provide the attributes of security, authentication, identity verification, trust, and privacy to a commonly accepted identification card for federal employees and contractors.

Recommendations

We recommend that DHS' Chief Security Officer, in conjunction with the Chief Information Officer:

Recommendation #1: Ensure that the PMO has the staffing and funding necessary to effectively coordinate and oversee the department-wide implementation of HSPD-12.

Recommendation #2: Develop a regional implementation plan that includes detailed information about how the PMO will centrally manage the department-wide deployment of its HSPD-12 program. The plan should identify milestone dates and define program measures to track HSPD-12 implementation progress.

Recommendation #3: Discuss and coordinate with OMB on the department's updated milestones and implementation of HSPD-12 requirements.

Recommendation #4: Estimate the department-wide cost to comply with HSPD-12 and FIPS 201-1 requirements and prioritize the department's costs to ensure that physical and logical access interoperability requirements will be met. The estimate should cover the funding and other resources necessary to support HSPD-12 over a period of no less than five years.

Recommendation #5: Identify the facility access points and information systems that will require the use of PIV cards.

Management Comments and OIG Analysis

DHS management concurred with recommendation 1. DHS noted, however, that the implementation of HSPD-12 has always been a priority for department leadership and the Management Directorate. To address the unfunded HSPD-12 mandate, department leadership took the initiative to realign existing resources (fiscal and personnel) from within the Office of the Chief Security Officer (OCSO) to provide funding and contractor support. Furthermore, OCSO is exploring the possibilities of detailing experienced and qualified component employees and an internal reorganization to obtain the necessary staffing. OCSO and the PMO will also work with the DHS Chief Financial Officer to identify a sustainable funding stream.

OIG Analysis

We do not agree with DHS' assertion that HSPD-12 has been a priority. In meetings held with management, DHS officials stated that HSPD-12, an unfunded mandate, was not previously a departmental priority. Therefore, funding was often diverted to higher priority programs, such as security background investigations. We do agree that current management, including the Secretary and Deputy Secretary, support the centrally managed approach and want HSPD-12 to be a priority because it helps create the “one DHS” strategy emphasized by unifying components.

The steps that DHS is taking, and plans to take, begin to satisfy this recommendation. We consider this recommendation resolved; it will remain open until DHS provides documentation to support that all planned corrective actions are completed.

DHS management concurred with recommendation 2. OCSO has developed a regional implementation plan using a centrally-purchased approach that includes oversight of the components’ implementation of HSPD-12. The plan, which will be finalized by January 30, 2010, will incorporate component input based on their anticipated certification and accreditation (C&A) schedules, as well as milestone dates and program implementation tracking measurements. Component completion of their respective C&A (i.e., Authority to Operate [ATO]) activities is a key dependency for DHS PIV card issuance. The OCSO centrally-purchased approach will use a component task force implementation model for card issuance. The component task force implementation model will rely on component staffing and active participation and management to carry-out their respective PIV issuance responsibilities. PIV card issuance is expected to begin in New York City; Dallas, TX; and Los Angeles, CA in the second quarter of FY 2010.

OIG Analysis

We agree that the steps that DHS is taking, and plans to take, begin to satisfy this recommendation. We consider this recommendation resolved; it will remain open until DHS provides documentation to support that all planned corrective actions are completed.

DHS management concurred with recommendation 3. Personnel from OCSO and OCIO met with OMB officials on November 18, 2009, to provide an update on the status of DHS HSPD-12 implementation. OMB was advised that the anticipated completion date is March 2012. This revised date is based on card issuance completion schedules, enterprise infrastructure progress, and the alignment of DHS efforts with the Federal Identity, Credential, and Access Management Roadmap and Implementation Guidance released on November 10, 2009.

OIG Analysis

We agree that the steps that DHS is taking, and plans to take, begin to satisfy this recommendation. We consider this recommendation resolved; it will remain open until DHS provides documentation to support that all planned corrective actions are completed.

DHS management concurred with recommendation 4. OCSO has developed a department-wide cost estimate for PIV deployment in FY 2010 that totals approximately $24 million. Efforts to quantify the totality of DHS HSPD-12 physical and logical access requirements are continuing. Component cost estimates are being consolidated to create a department-wide physical security cost estimate. This effort is scheduled to be completed in April 2010. Concurrent with this effort, the OCIO will develop a comprehensive cost estimate to implement logical access to DHS unclassified networks using HSPD-12 compliant PIV cards. OCIO anticipates completion of this effort by September 30, 2010. Finally, as part of the DHS Capital Planning and Investment Control process, Life Cycle Cost Estimates data developed for the DHS FY 2012 System Engineering Life Cycle planning and the OMB E300s will reflect the totality of the HSPD-12 physical and logical access interoperability requirements.

OIG Analysis

We agree that the steps that DHS is taking, and plans to take, begin to satisfy this recommendation. We consider this recommendation resolved; it will remain open until DHS provides documentation to support that all planned corrective actions are completed.

DHS management concurred with recommendation 5. In coordination with the DHS Physical Security Managers Working Group, the OCSO is consolidating component-provided inventories of physical access control systems and the identification of facility access points. By March 2010, OCSO expects to have a completed physical access control system roadmap. The roadmap will identify and prioritize facility access points, requirements, and identify the time-phase adaptation of legacy physical security environments to PIV-enabled and compatible environments. FIPS 201 compliant readers are currently being tested at locations around the Nebraska Avenue Complex (NAC). In particular, all employees entering the front gate of the NAC are required to use the PIV 201 reader. OCIO is reviewing all DHS information systems and will develop a comprehensive list of candidate systems for mandatory HSPD-12 PIV card access by September 30, 2010.

OIG Analysis

We agree that the steps that DHS is taking, and plans to take, begin to satisfy this recommendation. We consider this recommendation resolved; it will remain open until DHS provides documentation to support that all planned corrective actions are completed.

System, Account Management, and Physical Security Controls Are Not Effective

IDMS is DHS' contractor-developed and managed technical solution for PIV card issuance.[9] In September 2007, this solution received GSA approval as a FIPS 201 compliant card issuance system for identity proofing, records management, and credentialing of PIV smartcards. The contractor is responsible for maintaining the security over the system, including the IDMS database and card issuance workstations, training, and support. DHS' OCIO is currently overseeing the second option year of a five-year contract.

Headquarters PACS is an automated legacy system that DHS inherited from the Department of the Navy that manages PIV cardholder records and controls an individual's physical access to federally controlled Headquarters facilities, such as the NAC, through the use of card readers and applicable software. Card readers — electronic devices that supply power to and communicate with PACS and the PIV card — enable cardholders to be authenticated and communicate with the access control application.

We evaluated the physical and logical security controls implemented to determine whether they were effective in protecting the data collected and stored, including personally identifiable information (PII). We performed vulnerability testing of the IDMS database, web application, and server; government furnished equipment (GFE) at the contractor's Miami, FL, location and Headquarters enrollment centers; card issuance workstations located at Headquarters and CBP; and a kiosk located at the NAC. We also determined whether IDMS and PACS have been certified and accredited. In addition, we ran queries on the IDMS and PACS data to determine whether adequate account management and PIV card access controls have been implemented to restrict and control access to sensitive

[9] As documented in our 2007 report, the Identification and Credential Issuing Station and System (ICISS) was the predecessor to IDMS. Because ICISS could not be used to produce large quantities of PIV cards in a production environment, DHS sent out a proposal for a technical solution capable of meeting DHS' PIV card production requirements. IDMS was the system procured.

and personal data. Further, we tested a sample of PIV cards that had been revoked to determine whether they still allowed physical access to Headquarters facilities.

Overall, DHS has implemented adequate physical security controls over IDMS at the contractor facility in Miami. Physical security evaluations conducted at the Network Access Point of the Americas building and contractor headquarters offices in Miami, where the IDMS backup system is located, uncovered only a few minor issues. These issues were addressed by contractor's Facility Security Officer while on-site. However, our evaluations of physical security conducted at Headquarters card issuance and enrollment centers identified several security issues with regards to the protection of PIV card stock, PIV cards, and PII.

IDMS was certified and accredited to operate at the contractor's Miami site in June 2008, until becoming operational at the department's Stennis Data Center. The ATO for IDMS at the Stennis Data Center was granted in September 2009. Appendix D shows the overall architecture of IDMS and accreditation boundaries. Headquarters PACS has not been certified or accredited.

No high or critical system vulnerabilities were identified during our vulnerability assessments of the IDMS database, web application, and server. However, system security controls have not been implemented, and significant access control and account management security issues were identified.

Effective Security and Management Controls Have Not Been Implemented

A federal agency's success at managing its security requirements is contingent upon its processes for auditing governance, compliance, and use. Because many different users access an agency's facilities and networks, it is especially challenging for an agency to grant the necessary rights and privileges to each user while still protecting the confidentiality and privacy of its users and data. While privileges granted to PIV cardholders are a local agency decision, the PIV card is a core component to setting the "trust model" across the federal government.

DHS' oversight and implementation of security requirements and management controls were not effective. We identified issues surrounding system configuration management, separation of duties, biometric checking, the certification and accreditation of Headquarters PACS, account roles and privileges, and DHS PIV card controls.

System Security and Management Controls Are Not Enforced

Our assessment of IDMS identified a number of system security and management issues. We determined that system configuration management is not adequate and a number of security controls have not been implemented to protect personal data collected and processed by IDMS. We identified the following issues:

- The PMO is not enforcing a separation of duties when granting IDMS administrative account roles. Specifically, the PMO has chosen not to separate the roles of the enrollment official and PIV issuer via a "two-man rule," designed to segregate PIV card enrollment and issuer duties. When the two-man rule is implemented, the system would tag administrative account users who have enrolled an applicant and then tried to issue that applicant a PIV card by denying such an action.

  DHS chose not to implement a separation of duties through policy and system controls. Instead, the department implemented a seamless process where an employee visits only a single enrollment official. According to DHS officials, the department took this approach because it did not have enough enrollment staff to separate the roles.

  We identified 38 administrative account users who have both enrollment official and PIV issuer roles, meaning that these individuals have rights to enroll an applicant and issue a PIV card autonomously. Furthermore, 12 administrative account users have DHS PIV sponsor, PIV registrar, enrollment official, and PIV issuer roles. These roles allow them to create a new employee in the system, input card information, and then issue a card autonomously, increasing the risk that fraudulent cards may be produced and issued to unauthorized individuals.

  DHS' detailed PIV card and issuance roles are defined in Appendix C.

- Local logs on the Security Enhanced Linux (SELinux) server and GFE are inadequate. Furthermore, local logs are not reviewed on EIWS. Local logs on the EIWS are not protected from unauthorized modification, access, or destruction because users have local administrative privileges through a shared account.

- Password controls have not been implemented on the SELinux server that holds the IDMS database. In addition, the maximum password age was set to 99,999 days, while the minimum password age was set to 0 days.

- Required antivirus software was not installed on the EIWS.

The *Federal Identity Management Handbook* specifies that the approval authority should make sure that no single individual or role has the capability to issue a card without the participation of another individual; at least two different individuals must participate in the process at all times. A separation of duties is required by the *DHS Sensitive Systems Handbook 4300A* (DHS 4300A), for user access control. As documented in the *Department of Homeland Security (DHS) Headquarters Homeland Security Presidential Directive 12 (HSPD-12) Procedures Reference Book*, the DHS PIV sponsor should not be the PIV registrar or PIV issuer for the applicant.

Under DHS 4300A, configuration management controls must be established, implemented, and enforced on all information technology (IT) systems and networks. Logs (audit records) should contain enough detail to reconstruct an incident; logs are to be protected from unauthorized access, modification, and destruction. Furthermore, DHS policy requires the establishment and enforcement of virus protection control policies, which include the configuration and installation of antivirus software on servers. According to the DHS Linux Secure Baseline Configuration Guide (SBCG), a minimum password age should be set to seven days, and maximum password age should be set to 90 days.

DHS Is Not Performing Required Biometric Checks

DHS is not performing biometric checks during card registration and issuance. FIPS 201-1 requires that a full set of fingerprints be collected and compared with law enforcement data for biometric verification during the identity proofing and registration process. DHS has not been performing biometric checks during enrollment. DHS plans to leverage the department’s United States Visitor and Immigrant Status Indicator Technology system for biometric checks, but did not provide a timeframe for implementing the process to perform these checks. Identity proofing cannot be fully completed when fingerprint data is not compared with law enforcement data.

Headquarters PACS Has Not Been Certified and Accredited

Headquarters PACS is listed as in the "development" stage of the system development life cycle in Trusted Agent FISMA (TAF). However, PACS has been operational since November 2003 at the NAC, and used throughout the National Capital Region since April 2005. Therefore, PACS should be listed as an operational system, and certified and accredited to comply with DHS requirements implemented under the Federal Information Security Management Act (FISMA).

Headquarters PACS has not been certified and accredited. Accreditation is a formal declaration by a Designated Approving Authority that an information system is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk. To implement FISMA requirements, DHS requires system certification and accreditation prior to a system being operational.

Additionally, operational systems are to be listed in an agency's inventory according to OMB's FISMA reporting guidance. At DHS, systems that are in development in TAF are not counted toward system inventory. Because PACS should be listed as an operational system, DHS' system inventory is being underreported per OMB's FISMA reporting guidance.

Account and PIV Card Management Controls Have Not Been Defined

IDMS is composed of applications used to manage the identity verification, validation, and issuance processes to produce the department's PIV cards. The IDMS database contains records of all smartcards issued to employees and contractors, as well as their status. Much of this same sensitive information is contained in Headquarters PACS.

The activation and deactivation of DHS PIV cards in PACS is a manual process. Manual procedures are required because there is currently no electronic interface between the two databases. Once a card is issued via IDMS, cards must be activated in PACS to allow DHS Headquarters employees and contractors physical access to federally controlled facilities. Cards revoked in IDMS must be deactivated in PACS. The card issuance process is shown in Appendix E.

We performed detailed queries of IDMS to determine whether the administrative account access privileges to system data were properly controlled. Also, because the activation and deactivation of DHS PIV cards in PACS is a manual process, we compared card data in IDMS with Headquarters PACS data to determine whether the card status was updated properly in both systems. The results of our analysis showed:

- There are many unused and unaccounted for test accounts and cards currently active in IDMS. We also identified three user account roles — Applicant, Adjudicator, and Activator — that were assigned to 121 user accounts, but can no longer be used or granted to system users. Unused account roles should be deleted to prevent accidental or lingering access rights. According to DHS 4300A, unused user identifications should be disabled after 45 days of inactivity.

- There may be an excessive number of individuals with account access to the IDMS database and system audit logs. Our analysis identified 11 "su," or "super user," accounts, which grant full access to the IDMS database, and 18 Information System Security Officer (ISSO) accounts in IDMS, which allow the user to view and monitor system logs. The principle of least privilege must be implemented under DHS policy, and access to system logs should be restricted.

  According to DHS 4300A, the principle of least privilege must be applied to protect sensitive information and limit the damage that can result from accident, error, or unauthorized use. The principle of least privilege requires that users be granted the most restrictive set of privileges or lowest clearance needed to perform their authorized tasks. Users should be able to access only the system resources needed to fulfill their job responsibilities. The application of the least privilege principle ensures that access to sensitive information is granted only to those users with a valid need to know. Audit records and audit logs are to be protected from unauthorized modification, access, or destruction.

- Though the IDMS web application/database is compliant with DHS 4300A, we identified three web application accounts that were not assigned to specific individuals. Two were system accounts, used to initially set up the system and create administrative accounts; both of these accounts can no longer be used to access any information or establish new accounts. The third was a temporary test account that was never deleted.

Accounts that are not in use or have never been used should be deleted from the IDMS database.

- All IDMS EIWS users share one local administrator account. The shared account allows users more control of the system and limits the need for administrative personnel site visits to fix common issues, such as user account lockout. However, under DHS 4300A, shared accounts (i.e., such as group identifications and passwords) should be limited to operational necessity and must be approved by the appropriate Designated Approval Authority.

- The manual card deactivation process in use at DHS has led to inconsistencies between the IDMS and Headquarters PACS databases. Forty of the 1,539 deactivated cards, or 2.6%, were deactivated in IDMS but incorrectly left active in PACS. When physical access rights are still activated on a card, an individual may gain unauthorized access to DHS Headquarters facilities and areas.

- The contractor is not properly obtaining DHS permission to create or alter IDMS accounts. Although account management procedures have not been clearly defined, according to the IDMS System Security Plan, the contractor is to request permission to create or alter an account by sending an e-mail to either the HSPD-12 Program Manager or IT Lead. Once permission is granted, via another e-mail, contractor personnel can create or alter an account. Based on discussions with DHS and contractor personnel, permissions to create or alter IDMS accounts are usually requested in person or by phone. E-mails are not being sent to properly request permission as specified in the IDMS System Security Plan.

The need for formal procedures for properly creating, altering, and deleting accounts, and the informal creation of test records and accounts by contractor and DHS personnel, has led to a number of unused and unaccounted for card records in IDMS. The IDMS System Security Plan provides informal procedures for PIV cards and system access controls, but these procedures are not being followed by the contractor or enrollment officials, nor are they being enforced by the PMO. Because there is no electronic interface between IDMS and Headquarters PACS, the manual process used to update cards access privileges, activation, and deactivation, has led to inconsistencies between the two databases.

Authorized Signatory Agents Have Not Been Identified

The Office of Security's Headquarters Access Control Office (ACO) does not verify that an authorized signatory agent, or a person with the authority to grant an applicant's request for a DHS PIV card, signed an applicant's Access Control Card Request Form (DHS 11000-14). As long as Form 11000-14 is signed by a Special Security Officer (SSO), the ACO does not confirm whether the person that signed the applicant's form is authorized to approve an applicant's request.

The Headquarters ACO requires that each directorate submit a Signatory Authority Form every six months with the names of individuals authorized to sign off on the clearance portion of the Access Control Card Request Form. The ACO, however, has not developed a list of authorized signatory agents that are allowed to approve an applicant's DHS 11000-14 form or instituted verification procedures to ensure that forms are signed by authorized individuals.

Based on the Office of Security's Standard Operating Procedure, SSOs must sign all DHS 11000-14 forms for processing. However, according to the Headquarters ACO Branch Chief, SSOs only need to sign 11000-14 forms only for employees requiring a Top Secret/Sensitive Compartmented Information (TS/SCI) clearance. The SSO's signature is not necessary for applicants with other security clearance levels. It is unclear when an SSO is required to sign an applicant's DHS 11000-14 form.

Without a list of authorized signatory agents or clear standard operating procedures, there is an increased risk that unauthorized individuals may be approving applicants' forms and clearance information. Thereby, PIV issuers may be granting physical access to federally controlled facilities and areas containing TS/SCI and other classified information to individuals that may not need access.

Revoked PIV Cards Are Not Properly Tracked or Deactivated

ACO specialists at Headquarters enrollment centers are not properly tracking revoked or surrendered DHS PIV cards to ensure that the cards are promptly returned to the NAC ACO for physical destruction. According to the *Department of Homeland Security (DHS) Headquarters Homeland Security Presidential Directive 12 (HSPD-12) Procedures Reference Book*, a DHS PIV cardholder's supervisor is to notify the ACO when the cardholder no longer requires access to DHS facilities. Once the card has been received, the Headquarters ACO should promptly destroy the PIV card by shredding it and create a destruction report for the card.

The Headquarters ACO maintains a log of destroyed PIV cards. The destruction log includes the badge number, reason for destroying the card, date destroyed, the name of the individual who destroyed the card, and the name of a witness. However, the Headquarters ACO Branch Chief has not updated the destruction log on a regular basis. For example, when we requested the most recent destruction log on July 23, 2009, the ACO Branch Chief provided us with one dated March 23, 2009, as the most recent.

Also, ACO specialists are not deactivating DHS PIV cards in IDMS and Headquarters PACS in a timely manner. In testing a sample of 10 PIV cards having a status of "revoked" in IDMS, but not yet destroyed, 1 of the 10 revoked PIV cards still allowed physical access to Headquarters' 1120 Vermont Avenue facility. This card was still "active" in PACS. Additionally, though the cards obtained had a "revoked" status in IDMS, 4 of the 10 cards still have active certifications in IDMS.

We discussed our concerns with the Headquarters ACO Branch Chief. The Branch Chief has since taken steps to implement a new process at the 7th & D and NAC ACOs to ensure that all certifications are deactivated in IDMS, and the Headquarters PACS status is promptly deactivated. However, even with the new process in place, the security of DHS facilities, systems, and sensitive data may be compromised until there is an electronic interface between IDMS and PACS. This electronic interface would link IDMS and PACS so that any changes in one database would be reflected in the other in real-time, thereby reducing the risks associated with the current manual deactivation process.

Physical Security at Headquarters Needs Improvement

Our physical security evaluations conducted at two Headquarters ACOs exposed several issues with regard to the security of processing PIV cards and the protection of PII. At one ACO, our review uncovered that 11000-14 Identification Access Control Card Request forms that contain employee/contractor PII are stored in unlocked filing cabinets.

At the other ACO, blank PIV cards, 11000-14 forms, and cards that need to be destroyed are not being secured. Blank PIV cards and 11000-14 forms are stored in unlocked desk drawers at EIWS.

At the end of the workday, the enrollment officials consolidate all paper 11000-14 forms into a single folder and place the folder on top of a filing cabinet in the ACO; the folder containing the forms is not secured in any way. When a PIV card is surrendered, an enrollment official punches the PIV card chip out and stores the card in an EIWS desk drawer. Punching the PIV card chip out does not disable the magnetic strip, which stores a cardholder's physical access rights to Headquarters facilities.

According to the *Department of Homeland Security (DHS) Headquarters Homeland Security Presidential Directive 12 (HSPD-12) Procedures Reference Book*, the designated card custodian is responsible for storing card stock in a secure facility. The designated card custodian is also responsible for storing used, revoked, and defective PIV cards in a secure location until destruction. According to the *Federal Identity Management Handbook*, agencies should establish a business process and secure delivery method for all PIV-related documents. Regardless of the business process implemented by the agency, the process should be auditable and secure and should protect the applicant's PII.

Recommendations

We recommend that DHS' Chief Security Officer, in conjunction with the Chief Information Officer:

Recommendation #6: Address the configuration, card management, and user account issues identified according to HSPD-12 and DHS policy.

Recommendation #7: Develop a configuration management policy conducive to the department-wide deployment of EIWS at enrollment centers.

Recommendation #8: Develop formal procedures for creating IDMS accounts and roles, and the privileges associated with those accounts and roles.

Recommendation #9: Define account and PIV card management controls, procedures, and a process for ensuring that controls have been implemented.

Recommendation #10: Reconcile IDMS records with Headquarters PACS records to identify inconsistencies and ensure the accuracy of both databases.

Recommendation #11: Ensure that PACS is certified and accredited according to DHS policy under FISMA.

Recommendation #12: Define uniform, auditable policies and procedures that will clearly define when and how access controls should be properly granted and disabled, including card revocation, suspension, and destruction. These procedures should be established for all enrollment centers and implemented in all ACOs.

Recommendation #13: Establish an authorized signatory agent list and develop a procedure to verify signatures on DHS 11000-14 forms to ensure that only authorized individuals are signing DHS 11000-14 forms.

Recommendation #14: Develop detailed, uniform procedures that require enrollment center personnel to secure blank PIV cards, 11000-14 forms, and surrendered PIV cards containing PII while stored at the ACOs.

Recommendation #15: Implement procedures for evaluating physical security at ACOs and enrollment centers to ensure that PII is properly protected.

Management Comments and OIG Analysis

DHS management concurred with recommendation 6. The DHS HSPD-12 Procedures Reference Book will be revised by January 30, 2010, to incorporate new and additional policies, processes, and procedures, and system functionality, including configuration, card management, and user account issues. The revised reference book will also reflect system modifications and enhancements that have been made as a result of receiving ATO on September 11, 2009. As appropriate, this information will be incorporated into enrollment center training that will be provided to DHS PIV enrollment officials and ACO employees. Training requirements will also be included in solicitations that support nationwide deployment requirements.

OIG Analysis

We agree that the steps that DHS is taking, and plans to take, begin to satisfy this recommendation. We consider this recommendation resolved; it will remain open until DHS provides documentation to support that all planned corrective actions are completed.

DHS management concurred with recommendation 7. By January 30, 2010, the DHS HSPD-12 Procedures Reference Book will be revised to address the specific configuration management issues associated with department-wide deployment of the EIWS. Additionally, the reference book will updated to reflect feedback from the system's recent C&A process. As appropriate, this information will be incorporated into enrollment center training.

<u>OIG Analysis</u>

We agree that the steps that DHS is taking, and plans to take, begin to satisfy this recommendation. We consider this recommendation resolved; it will remain open until DHS provides documentation to support that all planned corrective actions are completed.

DHS management concurred with recommendation 8. By January 30, 2010, OCSO will update Section 2.0, *Roles and Responsibilities* of the DHS HSPD-12 Procedures Reference Book, to address the procedures for creating IDMS accounts and roles, and the privileges associated with those accounts and roles. As appropriate, this information will be incorporated into enrollment center training and audited by the PMO staff to ensure compliance.

<u>OIG Analysis</u>

We agree that the steps that DHS is taking, and plans to take, begin to satisfy this recommendation. We consider this recommendation resolved; it will remain open until DHS provides documentation to support that all planned corrective actions are completed.

DHS management concurred with recommendation 9. By January 30, 2010, OCSO will update Section 3.4, *DHS PIV Card Issuance, Re-Issuance, and Renewal* of the DHS HSPD-12 Procedures Reference Book, to define account and PIV card management controls, procedures, and a process for ensuring that controls have been implemented. As appropriate, this information will be incorporated into enrollment center training and audited to help ensure compliance.

<u>OIG Analysis</u>

We agree that the steps that DHS is taking, and plans to take, begin to satisfy this recommendation. We consider this recommendation resolved; it will remain open until DHS provides documentation to support that all planned corrective actions are completed.

DHS management concurred with recommendation 10. OCSO is establishing a methodology for reconciling daily Headquarters PIV card revocation reports from IDMS against activity in Headquarters PACS. The DHS Headquarters PACS interface is the first of its kind in the department and is therefore being used to define component requirements and technical integration requirements. Moreover, the Physical Security Manager's Working Group for PIV integration is documenting the common business processes and requirements that will form the basis for common department-wide standards and a sustainable enterprise-based technical solution.

OIG Analysis

We agree that the steps that DHS is taking, and plans to take, begin to satisfy this recommendation. We consider this recommendation resolved; it will remain open until DHS provides documentation to support that all planned corrective actions are completed.

DHS management concurred with recommendation 11. The PACS C&A process is underway and is scheduled for completion by the second quarter of FY 2010.

OIG Analysis

We agree that the steps that DHS is taking, and plans to take, begin to satisfy this recommendation. We consider this recommendation resolved; it will remain open until DHS provides documentation to support that all planned corrective actions are completed.

DHS management concurred with recommendation 12. By January 30, 2010, OCSO will update Section 3.0 *Procedures* of the DHS HSPD-12 Procedures Reference Book, to define uniform, auditable policies and procedures for granting, disabling, card revocation, suspension, and destruction. Additionally, the Physical Security Manager's Working Group for PIV integration is documenting the common business processes and requirements that will further define standard policies and procedures for enrollments centers and ACOs.

OIG Analysis

We agree that the steps that DHS is taking, and plans to take, begin to satisfy this recommendation. We consider this recommendation resolved; it will remain open until DHS provides documentation to support that all planned corrective actions are completed.

DHS management concurred with recommendation 13. The DHS OCSO ACO established a signatory agent list procedure in June 2005. In mid-2008, DHS Headquarters began exchanging legacy access control cards for HSPD-12 compliant PIV cards. To facilitate the issuance of the PIV card, the use of the signatory agent list was temporarily suspended for only those personnel who presented an unexpired legacy card. However, new employees and those that held a legacy access control card that was expired or lost, were still required to get an approved signatory authority's signature on the 11000-14. During the legacy card exchange period, signatory authority lists were periodically updated. The requirement for a properly signed DHS Form 11000-14 was reinstituted in October 2009, for all card issuance. OCSO will update the ACO's standard operating procedures and incorporate the updates into enrollment center and ACO training. The requirement is already included in the DHS HSPD-12 Procedures Reference Book, Section 3.3, *Adjudication and On-Boarding Determination*.

OIG Analysis

We agree that the steps that DHS is taking, and plans to take, begin to satisfy this recommendation. We consider this recommendation resolved; it will remain open until DHS provides documentation to support that all planned corrective actions are completed.

DHS management concurred with recommendation 14. By January 30, 2010, Section 3.0 of the DHS HSPD-12 Procedures Reference Book will be updated to more fully address the identification and protection of PII and to provide procedures for securing blank/surrendered PIV cards. OCSO will also reinforce current standard operating procedures and ensure enrollment center and ACO personnel are appropriately trained. When updating the reference book, standard operating procedures, and training, OCSO will refer to applicable DHS guidance, OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, and the Federal Identity, Credential, and Access Management Roadmap and Implementation Guidance.

OIG Analysis

We agree that the steps that DHS is taking, and plans to take, begin to satisfy this recommendation. We consider this recommendation resolved; it will remain open until DHS provides documentation to support that all planned corrective actions are completed.

DHS management concurred with recommendation 15. OCSO is strengthening existing standard operating procedures and training requirements associated with the physical security at ACOs. Storage containers, locks, and when applicable, alarms will be utilized at ACO locations. Furthermore, the DHS HSPD-12 Procedures Reference Book will be revised to more fully address physical security at the ACOs and the identification and protection of PII.

OIG Analysis

We agree that the steps that DHS is taking, and plans to take, begin to satisfy this recommendation. We consider this recommendation resolved; it will remain open until DHS provides documentation to support that all planned corrective actions are completed.

The objective of our audit was to determine whether DHS is meeting HSPD-12 implementation requirements and completing actions to address our prior audit recommendations. We determined whether DHS (1) adequately addressed HSPD-12 requirements in its implementation plan and process, (2) has implemented effective physical and system security controls to protect the privacy of personal data collected and processed by IDMS, and (3) completed system documentation in compliance with FISMA requirements.

Our audit focused on the requirements outlined in HSPD-12, *Policy for a Common Identification Standard for Federal Employees and Contractor*s; 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 201-1, *Personal Identity Verification (PIV) of Federal Employees and Contractors*. In addition, we reviewed the *Federal Identity Management Handbook*; *Department of Homeland Security (DHS) Headquarters Homeland Security Presidential Directive 12 (HSPD-12) Procedures Reference Book*; National Institute of Standards and Technology Special Publication (NIST SP) 800-53, *Recommended Security Controls for Federal Information Systems*; NIST SP 800-79-1, *Guidelines for the Accreditation of Personal Identity Verification Card Issuers*; *DHS Sensitive Systems Handbook 4300A*; DHS Windows SBCG; DHS Linux SBGG; and DHS Oracle SBCG.

We interviewed management personnel in the Office of Security and OCIO. In addition, we interviewed the HSPD-12 Program Manager, personnel from the Headquarters ACO, and contractor personnel, including the system administrators and the Facility Security Officer. Further, we interviewed Office of Inspector General security personnel and personnel from GSA's Managed Services Office.

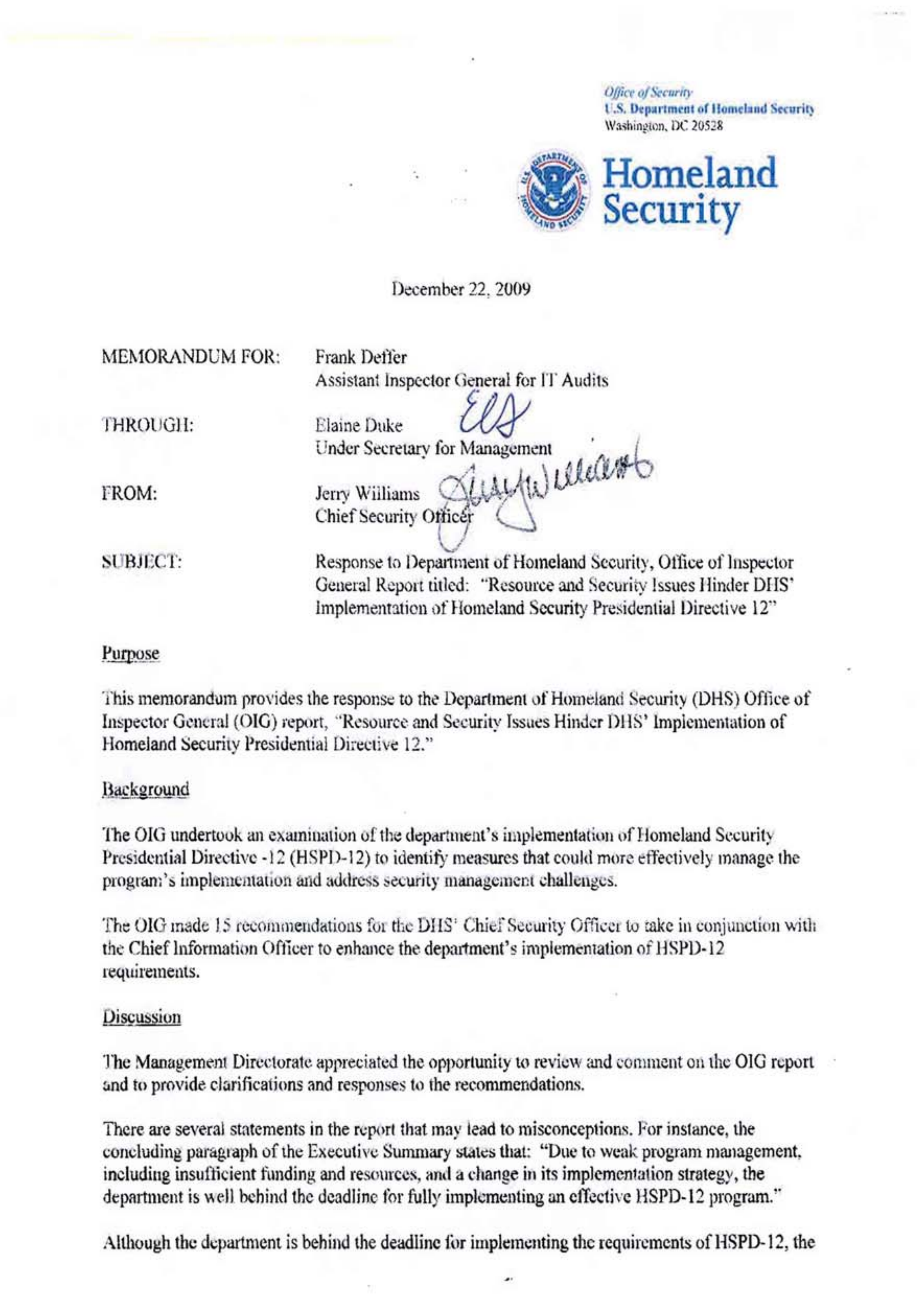
We evaluated DHS' HSPD-12 implementation plan, deployment process, and compliance with milestone dates. We conducted physical security evaluations of the contractor's facilities in Miami, FL, and the ACOs located in the Washington, DC, area. We also tested a sample of revoked PIV cards to determine whether they still allowed physical access to Headquarters facilities.

In addition, we performed detailed system security vulnerability assessments of the IDMS database, web application, and server; GFE at the contractor's Miami, FL, location and Headquarters enrollment centers; card issuance workstations located at Headquarters and CBP; and a kiosk located at the NAC. We excluded system security vulnerability testing of Headquarters PACS and an evaluation of the Virtual Private Network connection at the Stennis Data Center from our audit scope.

We verified account management controls and performed analytical queries of data contained in IDMS and Headquarters PACS. Furthermore, we analyzed certification and accreditation documentation for the IDMS and PACS systems. We followed up on prior recommendations made in our October 2007 report, *Progress Has Been Made But More Work Remains in Meeting Homeland Security Presidential Directive 12 Requirements* (OIG-08-01).

We conducted our fieldwork at DHS' Headquarters offices in the Washington, DC, metropolitan area and at contractor facilities in Miami, FL. Fieldwork was completed between June and October 2009 under the authority of the *Inspector General Act of 1978*, as amended, and according to generally accepted government auditing standards. Major OIG contributors to the audit are identified in Appendix F.

The principal OIG points of contact for the audit are
Frank W. Deffer, Assistant Inspector General, IT Audits, at
(202) 254-4100, and Edward G. Coleman, Director, Information Security Audit Division, at (202) 254 5444.



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

Homeland Security

December 22, 2009

MEMORANDUM FOR: Frank Deffer
Assistant Inspector General for IT Audits

THROUGH: Elaine Duke
Under Secretary for Management

FROM: Jerry Williams
Chief Security Officer

SUBJECT: Response to Department of Homeland Security, Office of Inspector General Report titled: "Resource and Security Issues Hinder DHS' Implementation of Homeland Security Presidential Directive 12"

Purpose

This memorandum provides the response to the Department of Homeland Security (DHS) Office of Inspector General (OIG) report, "Resource and Security Issues Hinder DHS' Implementation of Homeland Security Presidential Directive 12."

Background

The OIG undertook an examination of the department's implementation of Homeland Security Presidential Directive -12 (HSPD-12) to identify measures that could more effectively manage the program's implementation and address security management challenges.

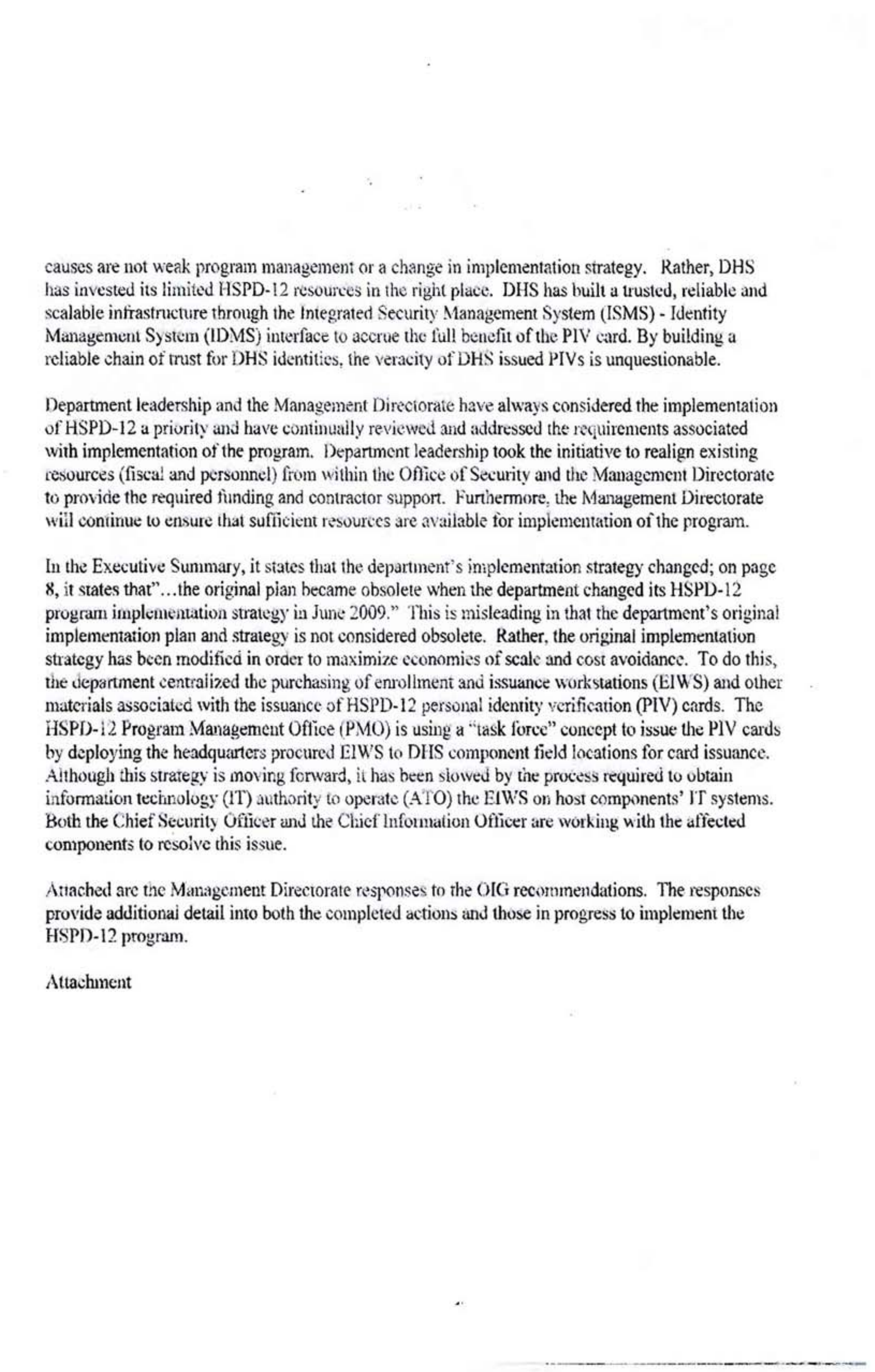
The OIG made 15 recommendations for the DHS' Chief Security Officer to take in conjunction with the Chief Information Officer to enhance the department's implementation of HSPD-12 requirements.

Discussion

The Management Directorate appreciated the opportunity to review and comment on the OIG report and to provide clarifications and responses to the recommendations.

There are several statements in the report that may lead to misconceptions. For instance, the concluding paragraph of the Executive Summary states that: "Due to weak program management, including insufficient funding and resources, and a change in its implementation strategy, the department is well behind the deadline for fully implementing an effective HSPD-12 program."

Although the department is behind the deadline for implementing the requirements of HSPD-12, the



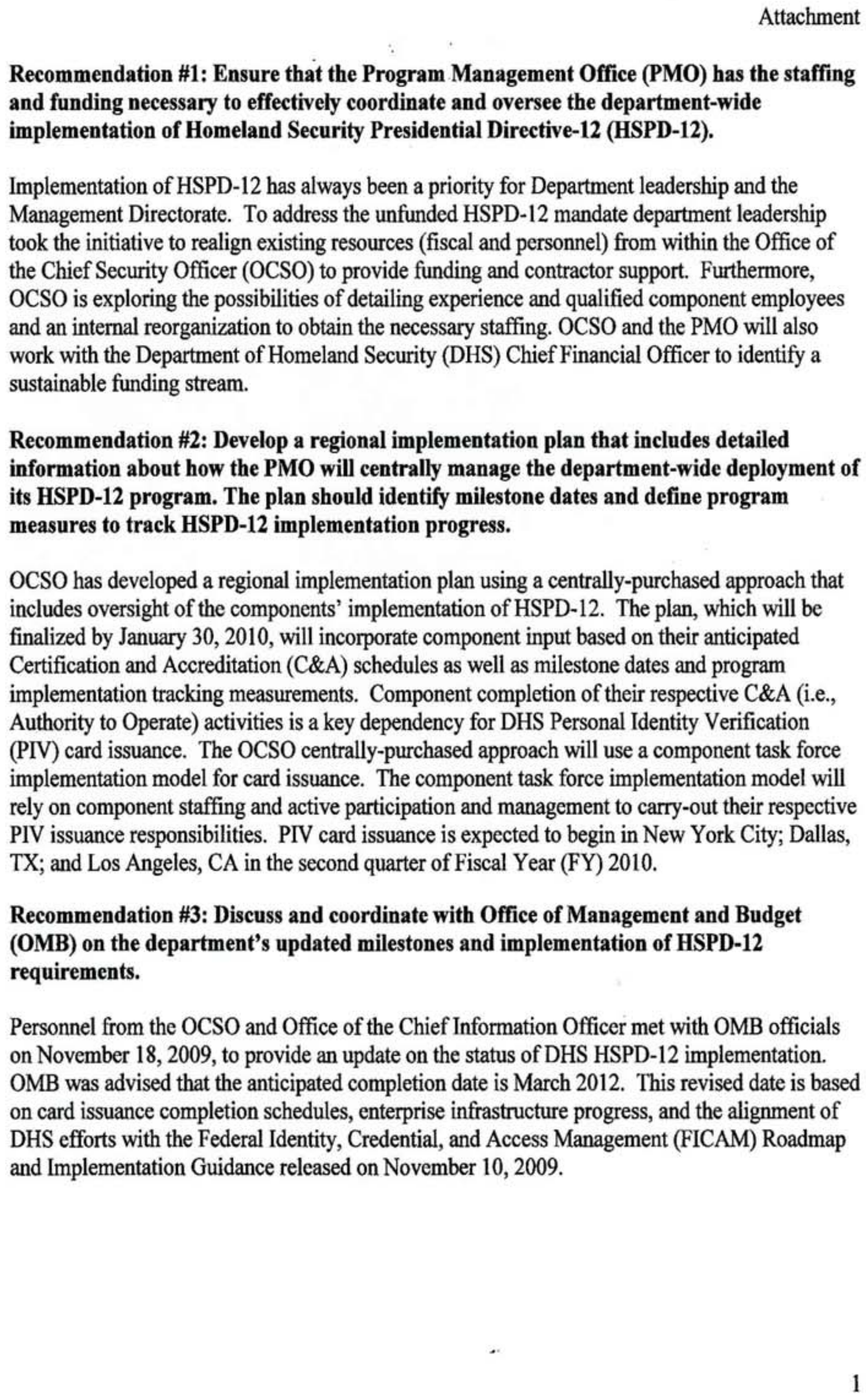
causes are not weak program management or a change in implementation strategy. Rather, DHS has invested its limited HSPD-12 resources in the right place. DHS has built a trusted, reliable and scalable infrastructure through the Integrated Security Management System (ISMS) - Identity Management System (IDMS) interface to accrue the full benefit of the PIV card. By building a reliable chain of trust for DHS identities, the veracity of DHS issued PIVs is unquestionable.

Department leadership and the Management Directorate have always considered the implementation of HSPD-12 a priority and have continually reviewed and addressed the requirements associated with implementation of the program. Department leadership took the initiative to realign existing resources (fiscal and personnel) from within the Office of Security and the Management Directorate to provide the required funding and contractor support. Furthermore, the Management Directorate will continue to ensure that sufficient resources are available for implementation of the program.

In the Executive Summary, it states that the department's implementation strategy changed; on page 8, it states that"…the original plan became obsolete when the department changed its HSPD-12 program implementation strategy in June 2009." This is misleading in that the department's original implementation plan and strategy is not considered obsolete. Rather, the original implementation strategy has been modified in order to maximize economies of scale and cost avoidance. To do this, the department centralized the purchasing of enrollment and issuance workstations (EIWS) and other materials associated with the issuance of HSPD-12 personal identity verification (PIV) cards. The HSPD-12 Program Management Office (PMO) is using a "task force" concept to issue the PIV cards by deploying the headquarters procured EIWS to DHS component field locations for card issuance. Although this strategy is moving forward, it has been slowed by the process required to obtain information technology (IT) authority to operate (ATO) the EIWS on host components' IT systems. Both the Chief Security Officer and the Chief Information Officer are working with the affected components to resolve this issue.

Attached are the Management Directorate responses to the OIG recommendations. The responses provide additional detail into both the completed actions and those in progress to implement the HSPD-12 program.

Attachment



Attachment

Recommendation #1: Ensure that the Program Management Office (PMO) has the staffing and funding necessary to effectively coordinate and oversee the department-wide implementation of Homeland Security Presidential Directive-12 (HSPD-12).

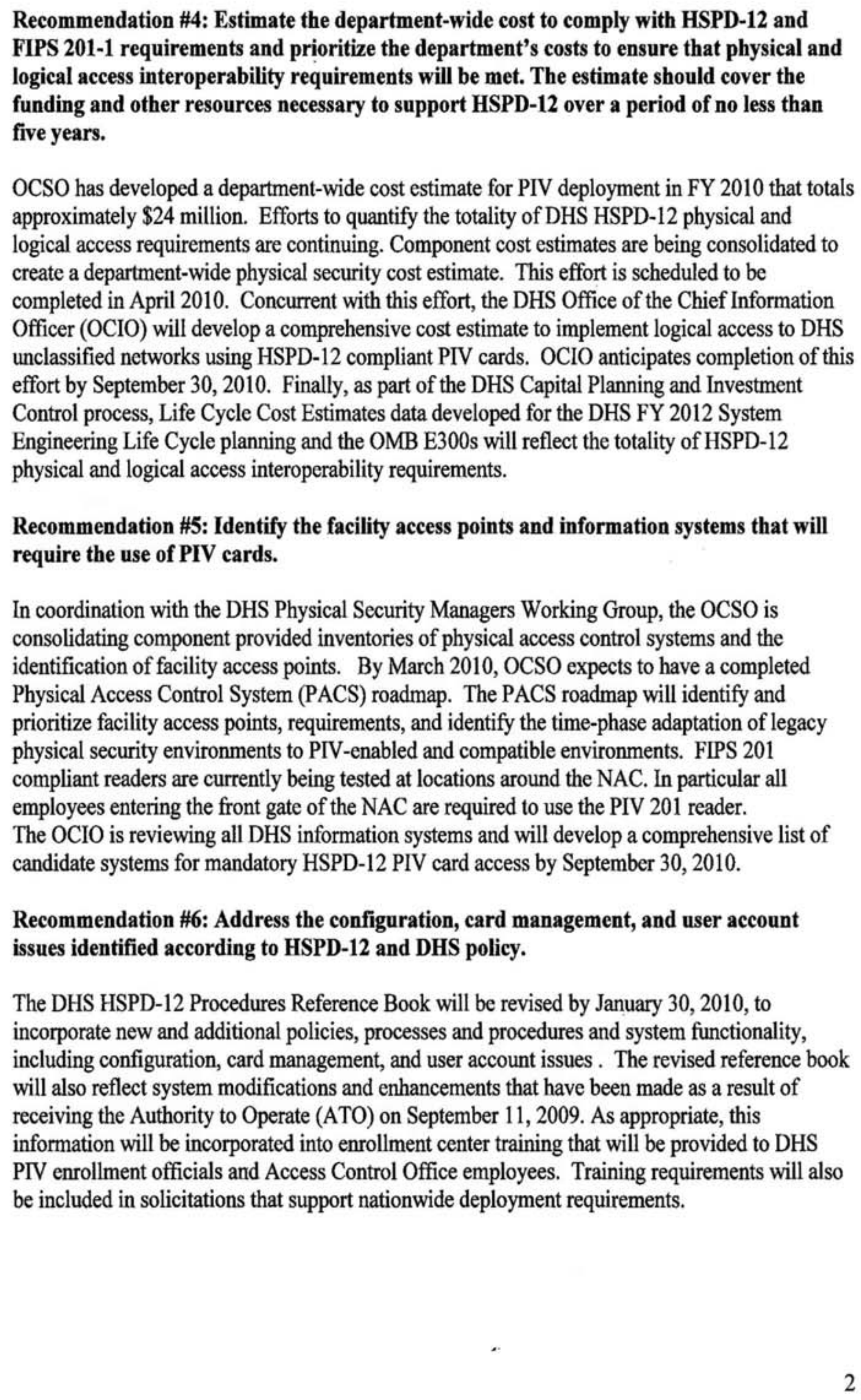
Implementation of HSPD-12 has always been a priority for Department leadership and the Management Directorate. To address the unfunded HSPD-12 mandate department leadership took the initiative to realign existing resources (fiscal and personnel) from within the Office of the Chief Security Officer (OCSO) to provide funding and contractor support. Furthermore, OCSO is exploring the possibilities of detailing experience and qualified component employees and an internal reorganization to obtain the necessary staffing. OCSO and the PMO will also work with the Department of Homeland Security (DHS) Chief Financial Officer to identify a sustainable funding stream.

Recommendation #2: Develop a regional implementation plan that includes detailed information about how the PMO will centrally manage the department-wide deployment of its HSPD-12 program. The plan should identify milestone dates and define program measures to track HSPD-12 implementation progress.

OCSO has developed a regional implementation plan using a centrally-purchased approach that includes oversight of the components' implementation of HSPD-12. The plan, which will be finalized by January 30, 2010, will incorporate component input based on their anticipated Certification and Accreditation (C&A) schedules as well as milestone dates and program implementation tracking measurements. Component completion of their respective C&A (i.e., Authority to Operate) activities is a key dependency for DHS Personal Identity Verification (PIV) card issuance. The OCSO centrally-purchased approach will use a component task force implementation model for card issuance. The component task force implementation model will rely on component staffing and active participation and management to carry-out their respective PIV issuance responsibilities. PIV card issuance is expected to begin in New York City; Dallas, TX; and Los Angeles, CA in the second quarter of Fiscal Year (FY) 2010.

Recommendation #3: Discuss and coordinate with Office of Management and Budget (OMB) on the department's updated milestones and implementation of HSPD-12 requirements.

Personnel from the OCSO and Office of the Chief Information Officer met with OMB officials on November 18, 2009, to provide an update on the status of DHS HSPD-12 implementation. OMB was advised that the anticipated completion date is March 2012. This revised date is based on card issuance completion schedules, enterprise infrastructure progress, and the alignment of DHS efforts with the Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance released on November 10, 2009.



Recommendation #4: Estimate the department-wide cost to comply with HSPD-12 and FIPS 201-1 requirements and prioritize the department's costs to ensure that physical and logical access interoperability requirements will be met. The estimate should cover the funding and other resources necessary to support HSPD-12 over a period of no less than five years.

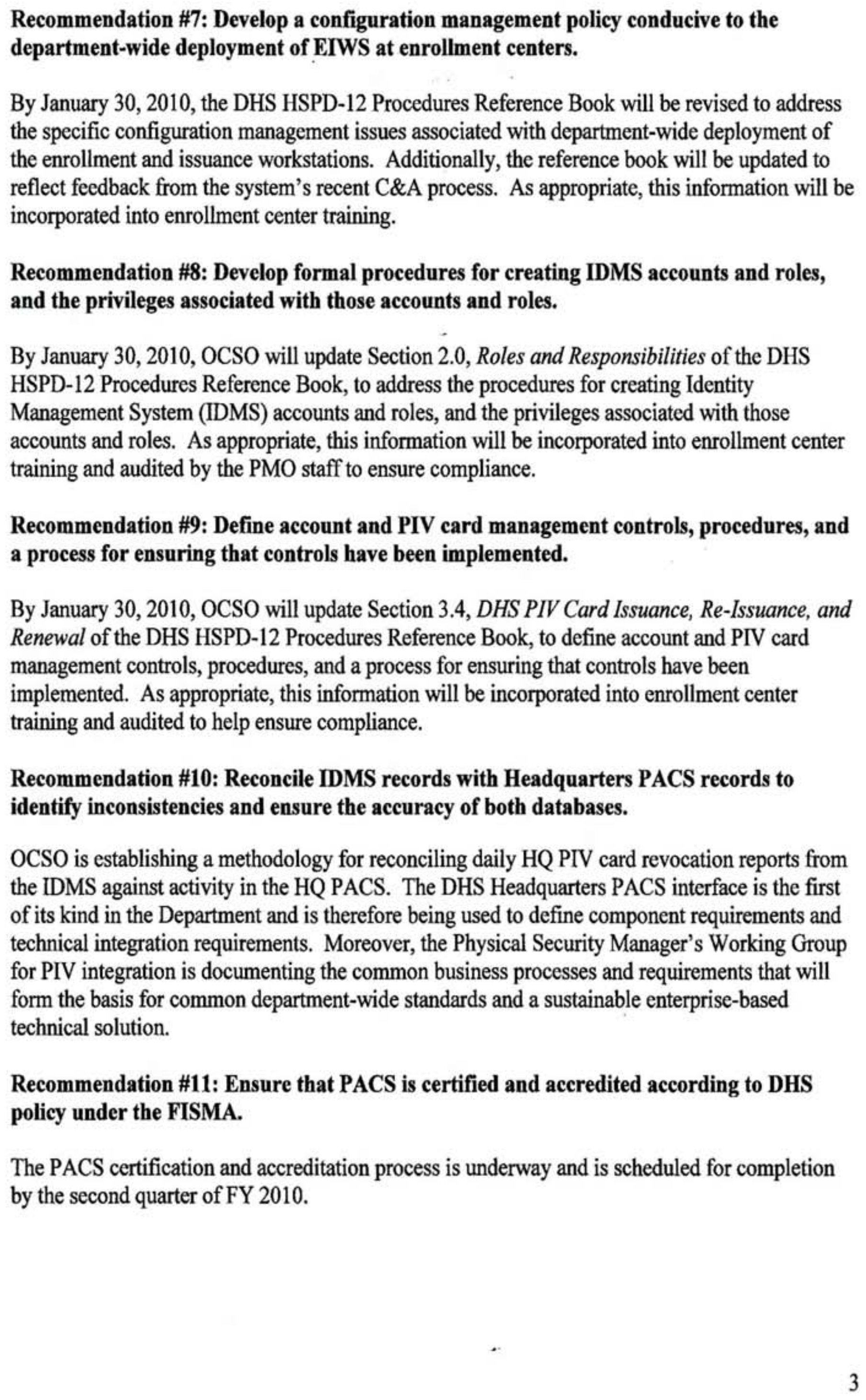
OCSO has developed a department-wide cost estimate for PIV deployment in FY 2010 that totals approximately $24 million. Efforts to quantify the totality of DHS HSPD-12 physical and logical access requirements are continuing. Component cost estimates are being consolidated to create a department-wide physical security cost estimate. This effort is scheduled to be completed in April 2010. Concurrent with this effort, the DHS Office of the Chief Information Officer (OCIO) will develop a comprehensive cost estimate to implement logical access to DHS unclassified networks using HSPD-12 compliant PIV cards. OCIO anticipates completion of this effort by September 30, 2010. Finally, as part of the DHS Capital Planning and Investment Control process, Life Cycle Cost Estimates data developed for the DHS FY 2012 System Engineering Life Cycle planning and the OMB E300s will reflect the totality of HSPD-12 physical and logical access interoperability requirements.

Recommendation #5: Identify the facility access points and information systems that will require the use of PIV cards.

In coordination with the DHS Physical Security Managers Working Group, the OCSO is consolidating component provided inventories of physical access control systems and the identification of facility access points. By March 2010, OCSO expects to have a completed Physical Access Control System (PACS) roadmap. The PACS roadmap will identify and prioritize facility access points, requirements, and identify the time-phase adaptation of legacy physical security environments to PIV-enabled and compatible environments. FIPS 201 compliant readers are currently being tested at locations around the NAC. In particular all employees entering the front gate of the NAC are required to use the PIV 201 reader.
The OCIO is reviewing all DHS information systems and will develop a comprehensive list of candidate systems for mandatory HSPD-12 PIV card access by September 30, 2010.

Recommendation #6: Address the configuration, card management, and user account issues identified according to HSPD-12 and DHS policy.

The DHS HSPD-12 Procedures Reference Book will be revised by January 30, 2010, to incorporate new and additional policies, processes and procedures and system functionality, including configuration, card management, and user account issues . The revised reference book will also reflect system modifications and enhancements that have been made as a result of receiving the Authority to Operate (ATO) on September 11, 2009. As appropriate, this information will be incorporated into enrollment center training that will be provided to DHS PIV enrollment officials and Access Control Office employees. Training requirements will also be included in solicitations that support nationwide deployment requirements.



Recommendation #7: Develop a configuration management policy conducive to the department-wide deployment of EIWS at enrollment centers.

By January 30, 2010, the DHS HSPD-12 Procedures Reference Book will be revised to address the specific configuration management issues associated with department-wide deployment of the enrollment and issuance workstations. Additionally, the reference book will be updated to reflect feedback from the system's recent C&A process. As appropriate, this information will be incorporated into enrollment center training.

Recommendation #8: Develop formal procedures for creating IDMS accounts and roles, and the privileges associated with those accounts and roles.

By January 30, 2010, OCSO will update Section 2.0, *Roles and Responsibilities* of the DHS HSPD-12 Procedures Reference Book, to address the procedures for creating Identity Management System (IDMS) accounts and roles, and the privileges associated with those accounts and roles. As appropriate, this information will be incorporated into enrollment center training and audited by the PMO staff to ensure compliance.

Recommendation #9: Define account and PIV card management controls, procedures, and a process for ensuring that controls have been implemented.

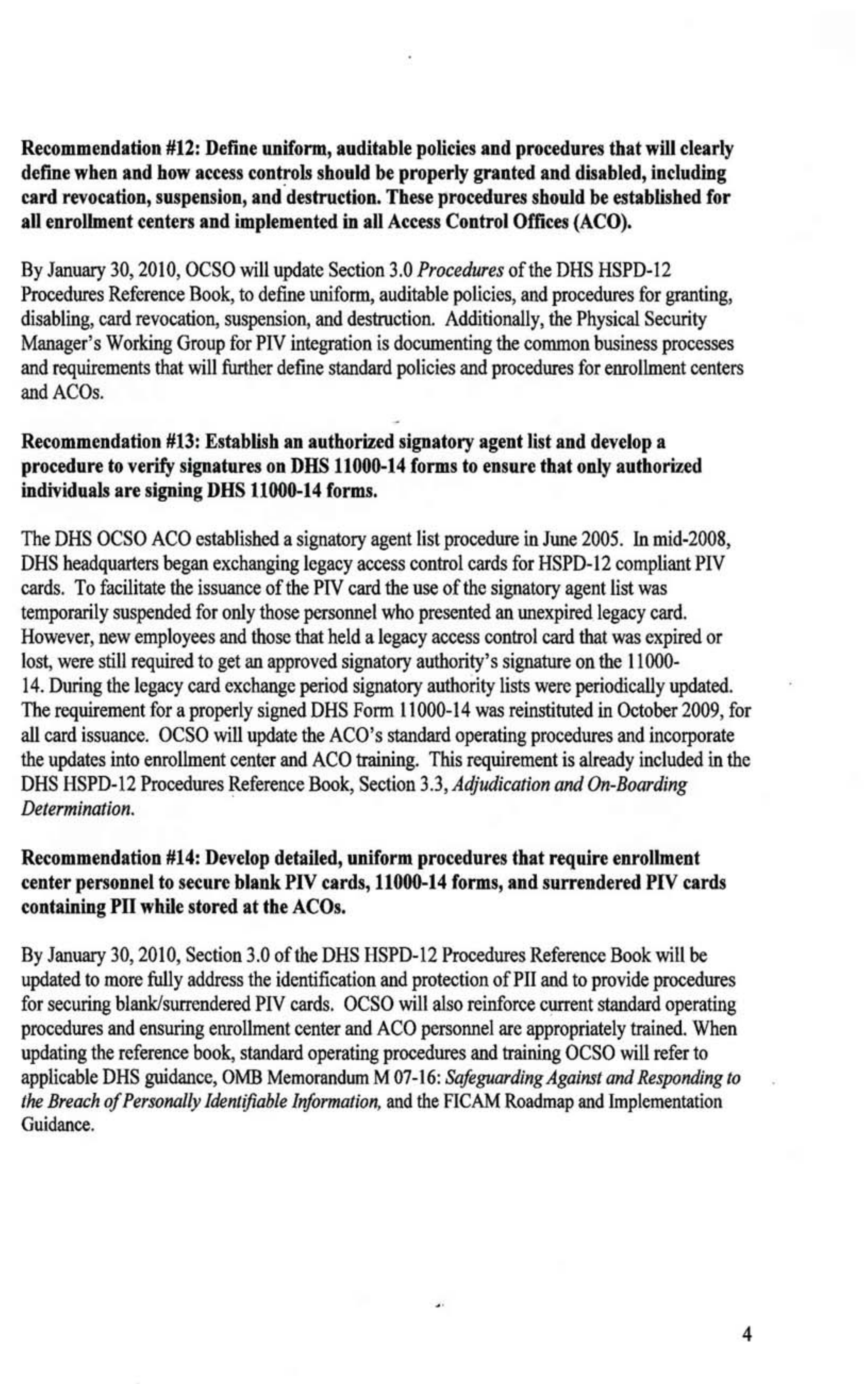
By January 30, 2010, OCSO will update Section 3.4, *DHS PIV Card Issuance, Re-Issuance, and Renewal* of the DHS HSPD-12 Procedures Reference Book, to define account and PIV card management controls, procedures, and a process for ensuring that controls have been implemented. As appropriate, this information will be incorporated into enrollment center training and audited to help ensure compliance.

Recommendation #10: Reconcile IDMS records with Headquarters PACS records to identify inconsistencies and ensure the accuracy of both databases.

OCSO is establishing a methodology for reconciling daily HQ PIV card revocation reports from the IDMS against activity in the HQ PACS. The DHS Headquarters PACS interface is the first of its kind in the Department and is therefore being used to define component requirements and technical integration requirements. Moreover, the Physical Security Manager's Working Group for PIV integration is documenting the common business processes and requirements that will form the basis for common department-wide standards and a sustainable enterprise-based technical solution.

Recommendation #11: Ensure that PACS is certified and accredited according to DHS policy under the FISMA.

The PACS certification and accreditation process is underway and is scheduled for completion by the second quarter of FY 2010.



Recommendation #12: Define uniform, auditable policies and procedures that will clearly define when and how access controls should be properly granted and disabled, including card revocation, suspension, and destruction. These procedures should be established for all enrollment centers and implemented in all Access Control Offices (ACO).

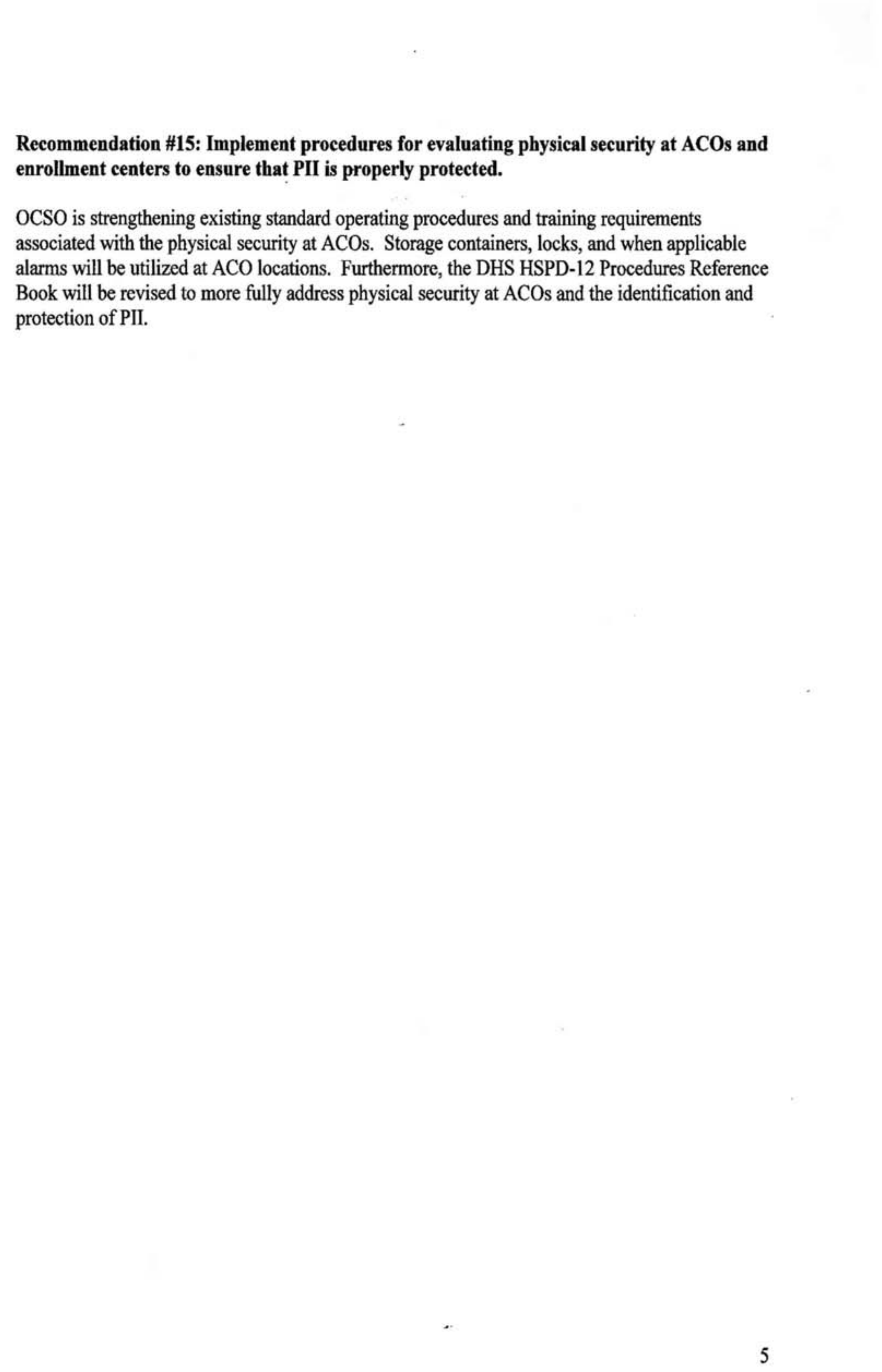
By January 30, 2010, OCSO will update Section 3.0 *Procedures* of the DHS HSPD-12 Procedures Reference Book, to define uniform, auditable policies, and procedures for granting, disabling, card revocation, suspension, and destruction. Additionally, the Physical Security Manager's Working Group for PIV integration is documenting the common business processes and requirements that will further define standard policies and procedures for enrollment centers and ACOs.

Recommendation #13: Establish an authorized signatory agent list and develop a procedure to verify signatures on DHS 11000-14 forms to ensure that only authorized individuals are signing DHS 11000-14 forms.

The DHS OCSO ACO established a signatory agent list procedure in June 2005. In mid-2008, DHS headquarters began exchanging legacy access control cards for HSPD-12 compliant PIV cards. To facilitate the issuance of the PIV card the use of the signatory agent list was temporarily suspended for only those personnel who presented an unexpired legacy card. However, new employees and those that held a legacy access control card that was expired or lost, were still required to get an approved signatory authority's signature on the 11000-14. During the legacy card exchange period signatory authority lists were periodically updated. The requirement for a properly signed DHS Form 11000-14 was reinstituted in October 2009, for all card issuance. OCSO will update the ACO's standard operating procedures and incorporate the updates into enrollment center and ACO training. This requirement is already included in the DHS HSPD-12 Procedures Reference Book, Section 3.3, *Adjudication and On-Boarding Determination.*

Recommendation #14: Develop detailed, uniform procedures that require enrollment center personnel to secure blank PIV cards, 11000-14 forms, and surrendered PIV cards containing PII while stored at the ACOs.

By January 30, 2010, Section 3.0 of the DHS HSPD-12 Procedures Reference Book will be updated to more fully address the identification and protection of PII and to provide procedures for securing blank/surrendered PIV cards. OCSO will also reinforce current standard operating procedures and ensuring enrollment center and ACO personnel are appropriately trained. When updating the reference book, standard operating procedures and training OCSO will refer to applicable DHS guidance, OMB Memorandum M 07-16: *Safeguarding Against and Responding to the Breach of Personally Identifiable Information,* and the FICAM Roadmap and Implementation Guidance.



Recommendation #15: Implement procedures for evaluating physical security at ACOs and enrollment centers to ensure that PII is properly protected.

OCSO is strengthening existing standard operating procedures and training requirements associated with the physical security at ACOs. Storage containers, locks, and when applicable alarms will be utilized at ACO locations. Furthermore, the DHS HSPD-12 Procedures Reference Book will be revised to more fully address physical security at ACOs and the identification and protection of PII.

5

DHS PIV Card and Issuance Roles

- **Applicant –** The individual applying for a DHS PIV card. The applicant must be a current or prospective federal hire, federal employee, or contractor.

- **DHS PIV Sponsor –** The individual responsible for administering the on-boarding for DHS Headquarters' new employees or contractors and initiating the identity vetting process. The sponsor is responsible for verifying that an individual should be obtaining a DHS PIV card, select the necessary system checks, and mark the sponsorship as approved. When new employees applying for a PIV card have not yet been entered into the Personnel Security Division's Integrated Security Management System, the sponsor has the ability to create a new record for the employee in the system. The sponsor, however, still needs to carry out the other responsibilities associated with the role prior to approving sponsorship.

- **Authorized Signatory Agent** – The individual authorized by a DHS directorate to approve the issuance of a DHS PIV card to an applicant.

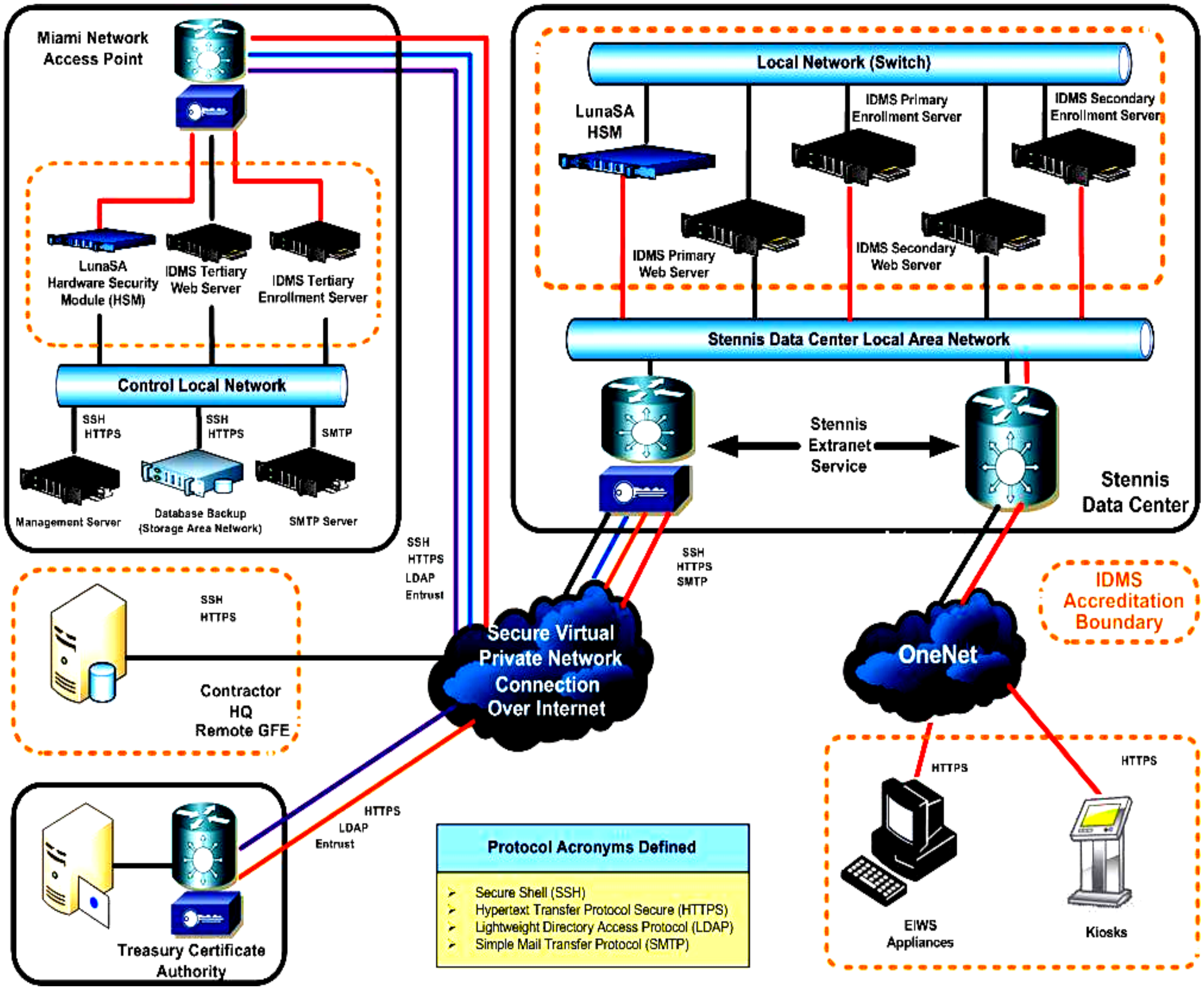
- **PIV Registrar –** The Personnel Security Division's Entry-on-Duty Adjudication team lead or the federal designee who makes the final determination for the applicant to proceed to DHS PIV card issuance. The registrar is responsible for the adjudication of background investigations and the Federal Bureau of Investigation check.

- **Enrollment Official –** The individual who initiates the chain of trust for identity proofing and provides trusted services to confirm employer sponsorship, bind the applicant to their biometric, and validate the identity source documentation. This official is responsible for obtaining an applicant's fingerprints, scanning identity documents, and capturing a photo of the applicant during the enrollment process.

- **PIV Issuer –** An authorized identity card creator that procures FIPS-approved blank identity cards, initializes them with the appropriate software and data elements for the requested identity verification and access control application, personalizes the cards with the identity credentials of authorized individuals, and delivers personalized cards to these individuals, along with appropriate instructions for protection and use. The issuer is responsible for printing, encoding, and activating the PIV card.

Appendix D
Current IDMS Architecture

Current IDMS Architecture



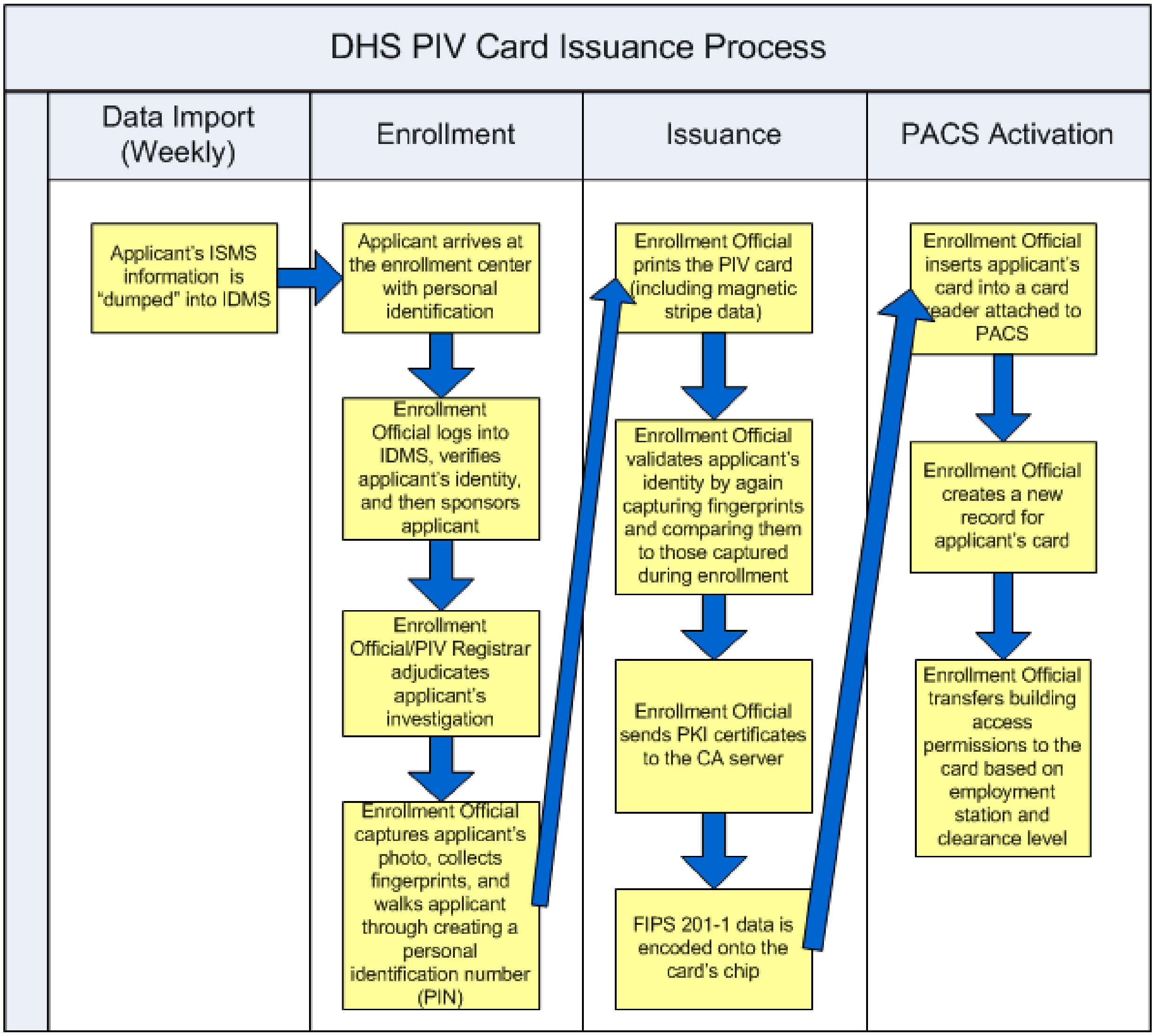
Miami Network Access Point
LunaSA Hardware Security Module (HSM)
IDMS Tertiary Web Server
IDMS Tertiary Enrollment Server
Control Local Network
SSH HTTPS
SSH HTTPS
SMTP
Management Server
Database Backup (Storage Area Network)
SMTP Server
SSH HTTPS LDAP Entrust
SSH HTTPS
Contractor HQ Remote GFE
Secure Virtual Private Network Connection Over Internet
HTTPS LDAP Entrust
Treasury Certificate Authority
Local Network (Switch)
LunaSA HSM
IDMS Primary Enrollment Server
IDMS Secondary Enrollment Server
IDMS Primary Web Server
IDMS Secondary Web Server
Stennis Data Center Local Area Network
Stennis Extranet Service
Stennis Data Center
SSH HTTPS SMTP
IDMS Accreditation Boundary
OneNet
HTTPS
HTTPS
EIWS Appliances
Kiosks

Protocol Acronyms Defined

- Secure Shell (SSH)
- Hypertext Transfer Protocol Secure (HTTPS)
- Lightweight Directory Access Protocol (LDAP)
- Simple Mail Transfer Protocol (SMTP)

Appendix E
DHS PIV Card Issuance Process

DHS PIV Card Issuance Process


DHS PIV Card Issuance Process
Data Import (Weekly)
Enrollment
Issuance
PACS Activation
Applicant's ISMS information is "dumped" into IDMS
Applicant arrives at the enrollment center with personal identification
Enrollment Official logs into IDMS, verifies applicant's identity, and then sponsors applicant
Enrollment Official/PIV Registrar adjudicates applicant's investigation
Enrollment Official captures applicant's photo, collects fingerprints, and walks applicant through creating a personal identification number (PIN)
Enrollment Official prints the PIV card (including magnetic stripe data)
Enrollment Official validates applicant's identity by again capturing fingerprints and comparing them to those captured during enrollment
Enrollment Official sends PKI certificates to the CA server
FIPS 201-1 data is encoded onto the card's chip
Enrollment Official inserts applicant's card into a card reader attached to PACS
Enrollment Official creates a new record for applicant's card
Enrollment Official transfers building access permissions to the card based on employment station and clearance level

Appendix F
Major Contributors to this Report

Information Security Audit Division

Edward Coleman, Director
Barbara Bartuska, IT Audit Manager
Mike Horton, IT Officer
Charles Twitty, IT Auditor/Team Lead
Bridget Glazier, IT Auditor
Amanda Strickler, IT Specialist
Tom Rohrback, IT Specialist
David Bunning, IT Specialist
Joseph Landas, Program and Management Clerk
Lauren Badley, Program and Management Clerk

Craig Adelman, Referencer

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff for Operations
Chief of Staff for Policy
Deputy Chiefs of Staff
General Counsel
Executive Secretariat
Director, GAO/OIG Liaison Office
Assistant Secretary for Office of Policy
Chief Security Officer
Deputy Chief Security Officer
Chief Information Officer
Chief Information Security Officer
Director, Compliance and Oversight Program
Chief, Identity Management Division
Chief Technology Officer, OCIO
Executive Director, IT Services Office (ITSO)
Deputy Director, Headquarters Services Division
Information System Security Manger, ITSO, Headquarters Services Division
Information System Security Officer, OCIO
Audit Liaison, OCIO
Director, OIG Information Security Audit Division
IT Audit Manager, OIG Information Security Audit Division

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees, as appropriate

ADDITIONAL INFORMATION AND COPIES

To obtain additional copies of this report, please call the Office of Inspector General (OIG) at (202) 254-4100, fax your request to (202) 254-4305, or visit the OIG web site at www.dhs.gov/oig.

OIG HOTLINE

To report alleged fraud, waste, abuse or mismanagement, or any other kind of criminal or noncriminal misconduct relative to department programs or operations:

- Call our Hotline at 1-800-323-8603;

- Fax the complaint directly to us at (202) 254-4292;

- Email us at DHSOIGHOTLINE@dhs.gov; or

- Write to us at:
  DHS Office of Inspector General/MAIL STOP 2600,
  Attention: Office of Investigations - Hotline,
  245 Murray Drive, SW, Building 410,
  Washington, DC 20528.

The OIG seeks to protect the identity of each writer and caller.