

DEPARTMENT OF HOMELAND SECURITY

Office of Inspector General

Progress Has Been Made But More Work Remains in Meeting Homeland Security Presidential Directive 12 Requirements



Office of Inspector General

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



**Homeland
Security**

October 15, 2007

Preface

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

This report addresses the progress DHS has made and the actions needed to comply with Homeland Security Presidential Directive 12 and implement Federal Information Processing Standards 201 requirements. It is based on interviews with employees and officials of relevant agencies and institutions, direct observations, 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. It is our hope that 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.

A handwritten signature in cursive script that reads "Richard L. Skinner".

Richard L. Skinner
Inspector General

Table of Contents/Abbreviations

Executive Summary	1
Background.....	2
Results of Audit	4
Actions Taken To Implement HSPD-12	4
Better Management of HSPD-12 Implementation Is Needed.....	7
DHS Is Behind In Its Implementation Schedule and May Not Meet OMB Milestones	7
Requirements for PIV Card Usage Have Not Been Determined	8
Costs to Implement HSPD-12 Have Not Been Assessed.....	9
Agency Head Has Not Accredited PIV-I Processes	10
PCI Services Must Be Re-accredited.....	10
Component Implementation Guidance Needs to be Updated.....	12
PIV Card Issuance Statistics Not Posted on Public Website	13
DHS Is Not Ready to Issue HSPD-12 Compliant Cards	14
PMO Needs to Bring Headquarters System to Production Readiness.....	14
Certification of ICISS Was Inadequate and Not Independent	15
Recommendations.....	16
Management Comments and OIG Analysis	17

Appendices

Appendix A: Purpose, Scope, and Methodology	19
Appendix B: Management Comments to the Draft Report	20
Appendix C: Example of a PIV Card	26
Appendix D: OMB Form I-9 Lists of Acceptable Documents	27
Appendix E: Major Contributors to this Report	28
Appendix F: Report Distribution.....	29

Table of Contents/Abbreviations

Abbreviations

DHS	Department of Homeland Security
FIPS	Federal Information Processing Standards
GSA	General Services Administration
HSPD-12	Homeland Security Presidential Directive 12
ICISS	Identification and Credential Issuing Station and System
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
OIG	Office of Inspector General
OMB	Office of Management and Budget
PCI	Personal Identity Verification Card Issuer
PIN	Personal Identification Number
PIV	Personal Identity Verification
PMO	Program Management Office
SP	Special Publication



Department of Homeland Security
Office of Inspector General

Executive Summary

We audited the Department of Homeland Security to determine whether the department has effectively managed the implementation of Homeland Security Presidential Directive 12 (HSPD-12). HSPD-12 requires the development and agency implementation of a mandatory, government-wide standard for secure and reliable forms of identification for federal employees and contractors. We determined whether the department's HSPD-12 implementation plan is adequate; policies and procedures to implement HSPD-12 requirements are adequate; and security controls implemented to protect the privacy of personal data collected and processed by HSPD-12 systems are effective.

The department has taken some actions to implement HSPD-12 requirements. For example, the department has established a Program Management Office to provide guidance and logistic support to implement HSPD-12 requirements at its headquarters and components. The Program Management Office developed a three-phase implementation plan and a procedures reference book that documents the processes to enroll applicants and issue credentials. Further, the Program Management Office prepared a privacy impact assessment providing details about personally identifiable information collected for issuing credentials. The privacy impact assessment described how the information may be accessed and how it will be securely stored. Furthermore, an HSPD-12 Council was established to facilitate the implementation of HSPD-12 throughout the department.

While the completion of these tasks helps the Department of Homeland Security fulfill some of its HSPD-12 requirements, more work remains. The department must devote further attention to ensure that it meets Office of Management and Budget established time frames for issuing HSPD-12 compliant cards to its employees and contractors. For example, the department is not scheduled to complete its HSPD-12 implementation until 2010, which is 2 years after the Office of Management and Budget's mandated deadline for all agencies. The department is also experiencing delays in implementing a technical solution and issuing compliant cards to its employees and contractors. In addition, the department has not assessed the total cost to implement HSPD-12 across the department and has not identified which facilities will require compliant cards in order to gain physical access, nor has it determined whether they will also be used for accessing information systems. Finally, the department must certify and accredit the headquarters and each component's personal identity verification card issuer service, as well as the information system that supports the service prior to implementation.

We are making seven recommendations to the Under Secretary for Management. While the department agreed to six of the recommendations, it did not concur with our recommendation to report its card issuance statistics on DHS' website. The department's response is summarized and evaluated in the body of this report and included, in its entirety, as Appendix B.

Background

On August 27, 2004, the President of the United States issued Homeland Security Presidential Directive 12 (HSPD-12), *Policy for a Common Identification Standard for Federal Employees and Contractors*. The purpose of HSPD-12 is to enhance security, increase government efficiency, reduce identity fraud, and protect personal privacy by establishing a mandatory, government-wide standard for secure and reliable forms of identification issued by the federal government to its employees and contractors (including contractor employees). In addition, HSPD-12 requires the Department of Commerce to promulgate a common standard for identification credentials, issued by federal departments and agencies for the purpose of gaining physical access to federally controlled facilities and logical access to federally controlled information systems.

On February 25, 2005, the National Institute of Standards and Technology (NIST) promulgated Federal Information Processing Standards (FIPS) 201, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, to satisfy the Department of Commerce's HSPD-12 requirement. FIPS 201 establishes the standard for secure and reliable forms of identification cards, performing background checks of government employees and contractors, and issuing identification cards used for entering government facilities and for accessing information systems. See Appendix C for an example of the front of a PIV card.

FIPS 201 is composed of two parts, PIV-I and PIV-II. PIV-I describes the minimum requirements for a federal personal identification system that meets the control and security objectives of HSPD-12, including personal identity proofing, registration, and issuance. PIV-II provides detailed technical specifications to support the control and security objectives in PIV-I, as well as interoperability of PIV cards and systems among federal departments and agencies.¹ The physical card characteristics, storage media, and data elements that make up identity credentials are specified in this standard. In addition, NIST has issued FIPS 201 companion publications that specify the interfaces and card architecture for storing and retrieving identity credentials from a

¹ PIV card is a smart card that contains stored identity credentials (e.g., a photograph, digital certificate and cryptographic keys, or digitized fingerprint representations) that is issued to an individual whose identity of the cardholder can be verified against the stored credentials by another person or through an automated process.

smart card, the requirements for collecting and formatting biometric information, PIV card application, and the interoperability between the card and reader.²

The Office of Management and Budget (OMB) is responsible for ensuring that agencies comply with HSPD-12. OMB issued memorandum M-05-24 on August 5, 2005 with instructions to federal agencies for implementing HSPD-12 and FIPS 201. According to OMB's M-05-04 instructions, the issuing of compliant cards to employees and contractors will be achieved in two phases with established milestones for each phase. Also included in its instructions to agencies, OMB emphasized that successful implementation of HSPD-12 and FIPS 201 would increase the security of federal facilities and information systems. OMB warned that inconsistent agency approaches to facility security and computer security are inefficient and costly, and increase risks to the federal government. Subsequently, OMB issued three memoranda with additional instructions to agencies on implementing HSPD-12.³ Figure 1 shows HSPD-12 implementation milestones.

Figure 1: HSPD-12 Implementation Milestones

Date	Requirements
October 27, 2005	Comply with PIV-I.
October 27, 2006	Comply with PIV-II.
October 27, 2007	Verify and/or complete background investigations and issue PIV cards for all employees with less than 15 years of government service.
October 27, 2008	Verify and/or complete background investigations and issue PIV cards for all employees with more than 15 years of government service.

The General Services Administration (GSA), in collaboration with the Federal Identity Credentialing Committee, the Federal Public Key Infrastructure Policy Authority, OMB, and the Smart Card Interagency Advisory Board developed the *Federal Identity Management Handbook*. This handbook aids agencies in implementing HSPD-12 and FIPS 201, and includes guidance on specific courses of action, schedule requirements, acquisition planning, migration planning, lessons learned, and case studies. In addition, GSA issued a memorandum on August 10, 2005 to agency officials that specified standardized procedures for acquiring FIPS 201-compliant commercial

² Smart card is a tamper-resistant security device, which is about the size of a credit card, and relies on an integrated circuit chip for information storage and processing.

³ M-06-06, Sample Privacy Documents for Agency Implementation of Homeland Security Presidential Directive (HSPD) 12, February 17, 2006; M-06-18, Acquisition of Products and Services for Implementation of HSPD-12, June 30, 2006; and M-07-06, Validating and Monitoring Agency Issuance of Personal Identity Verification Credentials, January 11, 2007.

products that have passed NIST's conformance tests. According to the GSA guidance, agencies are required to use standardized acquisition procedures when implementing their FIPS 201 compliant systems. In addition, GSA also offers a shared services solution to federal agencies that includes enrollment, identity management, card management, card production (printing and personalization), public key infrastructure, and issuance. Background investigations, system integration, physical access control systems, and logical access control systems remain the responsibility of the participating agencies.

The Office of Security leads the department-wide program for implementation of HSPD-12. The Office of the Chief Information Officer (OCIO) is responsible for the technical aspects of the program. The DHS Office of Security established the headquarters HSPD-12 Program Management Office (PMO) in March 2006, with the mission to implement HSPD-12 at headquarters and to guide component implementation efforts across DHS.⁴ The PMO consists of a program manager and six staff (one federal employee, five contractors). The PMO is responsible for implementing a process to issue PIV cards to approximately 70,000 headquarters employees and contractors. The remaining eight components are responsible for issuing PIV cards to their own approximately 140,000 employees and contractors.⁵ According to the PMO program manager, the United States Coast Guard is exempted from the requirement to use the technical solution developed at headquarters, as it will issue Department of Defense's PIV cards.

Results of Audit

Actions Taken To Implement HSPD-12

DHS has taken several actions to implement HSPD-12 requirements. The PMO developed an implementation plan that details the objectives, priorities, parameters, and outputs to achieve its mission and enable DHS to comply with HSPD-12 requirements. The plan also details a schedule and outlines those actions that must take place in order to implement HSPD-12 at DHS headquarters. The PMO has worked collaboratively with the OCIO to develop requirements and policies, and to implement the technical solution to issue HSPD-12 compliant cards. In addition, the PMO is providing guidance and tools to help facilitate the components' implementation of HSPD-12. The

⁴ For HSPD-12 implementation, DHS defines headquarters as the offices and components that are currently issued security badges by the DHS Office of Security, such as Management, Science and Technology, United States Visitor and Immigrant Status Indicator Technology, and Office of Inspector General. The remaining eight components, Customs and Border Protection, Citizenship and Immigration Services, Federal Emergency Management Agency, Federal Law Enforcement Training Center, Immigration and Customs Enforcement, Transportation Security Administration, United States Coast Guard, and United States Secret Service are responsible for implementing HSPD-12 at their components.

⁵ It is reported in OMB's *FY 2006 Report to Congress on Implementation of the Federal Information Security Management Act of 2002* that DHS has 207,776 employees and contractors.

components are responsible for creating their own implementation plan based on their unique circumstances and will use DHS headquarters processes and its technical solution.

According to the PMO’s plan, DHS will implement HSPD-12 in three phases. Figure 2 graphically shows DHS’ implementation approach.

- **Phase I-DHS Headquarters Implementation** At DHS headquarters, the PMO implements policies, procedures, and other supporting tasks, not included in the OCIO's HSPD-12 responsibilities, to comply with HSPD-12. This phase establishes the baseline from which lessons learned and best practices are developed for later phases. Phase I started in May 2006.
- **Phase II-Component Rollout** HSPD-12 rolls out to the components. The components assess their HSPD-12 requirements, develop, or update their policies and procedures, construct or select their PIV card issuance systems, and implement HSPD-12 solutions, enabling the department to achieve compliance. Phase II started in January 2007.
- **Phase III-Legacy Cardholder Migration** This final phase facilitates the conversion of current employees and contractors from holding existing DHS badges to receiving PIV-compliant badges. Phase III is estimated to begin in December 2007.

Figure 2: Phases of DHS’ Implementation of HSPD-12

Phase I	Phase II	Phase III
DHS HQ Implementation	Component Rollout	Legacy Cardholder Migration
Comply with HSPD-12 at the HQ level to develop the baseline framework for other components.	Rollout HQ HSPD-12 compliance framework to components and guide compliance across DHS.	Convert legacy contractors and employees from the existing DHS badges to PIV compliant badges.

DHS also took other actions:

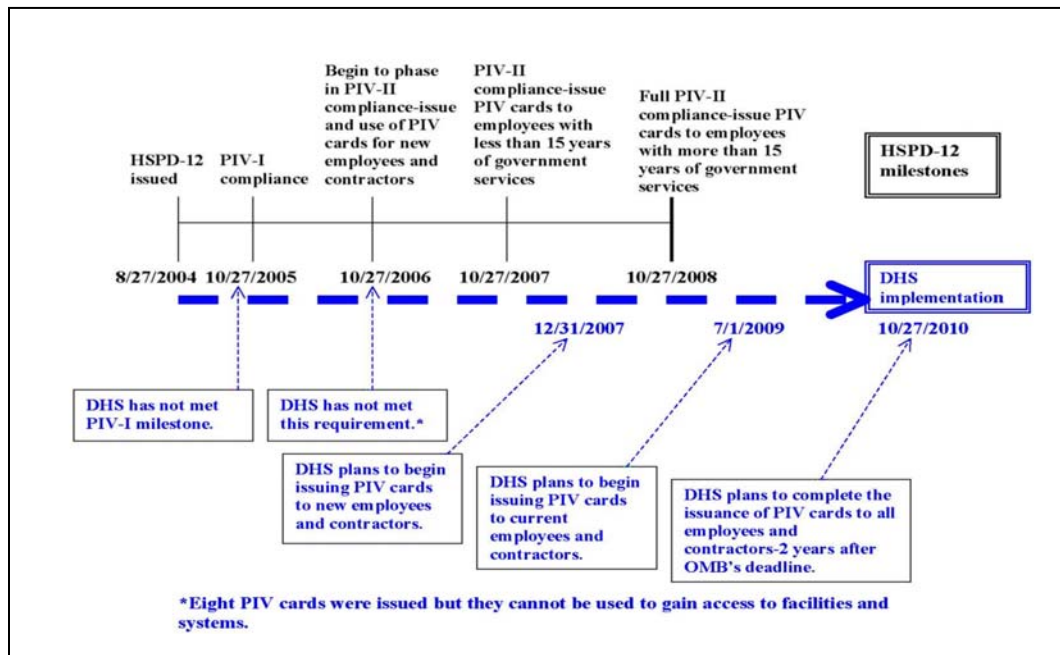
- The PMO developed a *Component Implementation Guidance Package*, which includes the *DHS Headquarters HSPD-12 Procedures Reference Book* that documents the process to enroll applicants and issue PIV cards.
- The PMO prepared a privacy impact assessment, dated October 13, 2006, to detail what personally identifiable information, used for issuing credentials and meeting HSPD-12 requirements, is

being collected, why it is being collected, how the information will be used and shared, how the information may be accessed, and how it will be stored securely.

- The PMO established an HSPD-12 Council, with representatives selected by the Chief Security Officer from each component, to facilitate the implementation of HSPD-12 throughout the department.
- DHS’ public key infrastructure has been cross-certified with the Federal Bridge Certification Authority to ensure that all digital certificates for the PIV cards are issued under the Federal Common Policy.⁶
- DHS provided its PIV card to GSA for testing, as required by OMB. GSA verified that the card met FIPS 201 requirements.

The completion of these tasks fulfills some of the HSPD-12 requirements. However, DHS is experiencing delays. More work remains to ensure that DHS is fully compliant with HSPD-12 and OMB-established timeframes and requirements for developing a technical solution and issuing PIV cards to its employees and contractors. See Figure 3 for OMB milestones and DHS timeline.

Figure 3: OMB Milestones and DHS Timeline



⁶ The public key infrastructure is a combination of products, services, facilities, policies and procedures, agreements, and people that provide for and sustain secure interactions on open networks such as the Internet. The public key infrastructure uses a security technique called Public Key Cryptography to authenticate users and data, protect the integrity of transmitted data, and ensure the non-repudiation and confidentiality of data.

Better Management of HSPD-12 Implementation Is Needed

DHS has not effectively managed the implementation of its HSPD-12 program to ensure that the department can meet all mandated milestones. DHS has not completed the actions needed to finish Phase I of its implementation plan and comply with PIV-I and PIV-II requirements. Specifically, DHS has not identified the requirements for the usage of PIV cards and determined its total costs to implement HSPD-12. In addition, DHS has not accredited its PIV-I process or its PIV card issuance service. Further, DHS has not provided its components with sufficient guidance for their individual implementation of HSPD-12, and has not complied with OMB implementation reporting instructions.

DHS Is Behind In Its Implementation Schedule and May Not Meet OMB Milestones

DHS' implementation schedule does not ensure that the department will be HSPD-12 compliant within OMB's established timeline. Federal agencies are required to phase in the issuance and use of PIV cards for all new employees and contractors by October 27, 2007, and complete the issuance of PIV cards to all employees by October 27, 2008. DHS is not scheduled to complete its HSPD-12 implementation until 2010, which is 2 years after the mandated deadline for all agencies, as stated in OMB memorandum M-05-04.

PMO officials maintain in their implementation plan that DHS is transitioning from Phase I to Phase II. In order to complete the implementation of Phase I, DHS was to have accomplished key tasks, such as assess costs, initiate component support, bring the headquarters system to production readiness, and begin PIV card issuance at headquarters. However, DHS has completed only its initiation of component support, one of its four key tasks. The department is experiencing delays in developing a technical solution capable of interfacing with other existing external and internal DHS systems and is therefore unable to issue PIV cards to its employees and contractors. The PMO has reported to OMB that it has completed Phase I of its implementation plan.

According to its Phase II implementation, DHS is scheduled to begin issuing PIV cards to new headquarters employees and contractors by December 2007, and components are to begin to issue PIV cards to their new employees and contractors by January 2008. DHS plans to use a contractor to develop its production system. However, as of July 2007, no award has been made. For Phase III implementation, DHS and its components are scheduled to begin issuing PIV cards to current employees and contractors in July 2009 and ending September 2010.

According to program officials, OMB concurred with DHS' extended timetable for HSPD-12 implementation. OMB's Deputy General Counsel confirmed that DHS had been granted an extended timetable to implement HSPD-12. Specifically, OMB approved the following extended milestones for DHS:

- Begin issuing PIV cards to employees and contractors in December 2007.
- Complete issuing PIV cards to 80% of the workforce by December 2008.
- Complete issuing PIV cards to the remaining 20% of the workforce by December 2010.

Even with OMB's extension, the department's current implementation schedule does not guarantee that DHS and its components will meet OMB's milestones to issue PIV cards to 80% of its workforce (approximately 168,000 employees and contractors) by December 2008. Based on its implementation plan, DHS and its components only plan to issue PIV cards to new employees and contractors in 2008 and are not scheduled to issue PIV cards to the majority of its workforce (current employees and contractors) until July 2009. Furthermore, DHS will not have the capability to issue PIV cards to its employees and contractors until its new production system becomes operational. According to program officials, the new technical solution is planned to be operational in December 2007.

Requirements for PIV Card Usage Have Not Been Determined

DHS and its components have not identified to what extent PIV cards will be used or required in order to access facilities or information systems throughout the department. DHS has not determined which facilities will require PIV cards in order to gain physical access, whether PIV cards will be used for accessing information systems, and which systems will be affected.

The determination as to the usage of PIV cards is important because the cards will be personalized in order to perform identity verification both by people and by automated systems. People can use the physical card for visual comparisons and automated systems can use the electronically stored data on the card to conduct automated identity verification. Without determination of usage, DHS may have to upgrade its infrastructure; procure additional equipment, for example, card readers; or make modifications to the PIV cards to include additional information after the cards are issued.

Costs to Implement HSPD-12 Have Not Been Assessed

To comply with PIV-II, agencies were required to demonstrate their ability to issue PIV cards by October 27, 2006. By this date, agencies were further tasked to begin to issue and require the use of PIV cards for all new employees and contractors. To assist agencies in meeting these timeframes, GSA established a shared services solution, which all federal agencies could use that includes registering employees and contractors, verifying their identities, and producing and issuing PIV cards.

GSA provides a complete solution for the enrollment, production, finalization, and on-going maintenance of HSPD-12 compliant credentials. Participating agencies who sign up with GSA receive an identity account for each cardholder with a secure HSPD-12 compliant credential; four public key infrastructure certificates; two fingerprint templates; secure backend cardholder and card management system; a nation-wide network of fixed and mobile enrollment stations shared by all participating agencies; help desk and maintenance support for the credential; and secure entry of personnel into the system. Additionally, GSA will provide all acquisition, financial and program management services. GSA is also responsible for the security and accreditation of the system.

GSA had originally estimated that it would charge federal agencies \$110 (plus an annual maintenance fee of \$52) to issue a PIV card. GSA revised its estimate in June 2007 and lowered the cost to \$82 per PIV card (plus an annual maintenance fee of \$36). Using GSA's revised estimate, it would cost DHS approximately \$17 million to issue PIV cards to its roughly 210,000 employees and contractors with an annual maintenance fee of \$7.5 million.

DHS decided not to use the GSA's solution. DHS envisioned interfacing three of its existing systems, which supported current initiatives in identity management, public key infrastructure, and the use of smart cards as its technical HSPD-12 solution. DHS officials believed the department could enhance, upgrade, and interface with these existing systems to issue PIV cards at a cost lower than GSA's shared services solution. However, DHS did not perform a cost benefit analysis to support its decision not to use GSA's solution.

As of May 2007, DHS has not developed cost projections for implementing HSPD-12 at its headquarters and components. The PMO has budgeted approximately \$1.5 million to implement HSPD-12 at the headquarters for fiscal year 2008 to cover PMO salaries, contract services, and the purchase of PIV cards. The remaining eight components have yet to develop their own cost estimates or budgets necessary to implement HSPD-12.

Without developing a total estimate, DHS does not know the most cost effective solution and places in jeopardy its implementation of HSPD-12. Further, DHS has not determined whether it has allocated enough resources to issue PIV cards to its employees and contractors. For example, DHS and its components will be required to purchase the hardware and software necessary to issue PIV cards. Furthermore, DHS may have to allocate additional resources to replace existing card readers with newer models for physical access and upgrade network infrastructure for accessing to information systems that are compatible with the PIV cards. Since the planned use of PIV cards throughout the department has not been determined, DHS does not know how many new card readers are needed to replace existing equipment and cannot assess the complete cost to implement HSPD-12.

Agency Head Has Not Accredited PIV-I Processes

The Secretary has not accredited the two PIV-I processes. Agencies were required to comply by October 27, 2005, with the first HSPD-12 milestone (PIV-I).

To satisfy the PIV-I milestone, agency heads were required to adopt and accredit (1) an identity proofing and registration process, and (2) a PIV card issuance and maintenance process. The identity proofing and registration process refers to the collecting, storing, and maintaining of all information and documentation that is required for verifying and assuring the applicant's identity. The card issuance and maintenance process should include standardized specifications for printing photographs, names, and other information on PIV cards; loading relevant electronic applications into a card's memory; capturing and storing biometric and other data; issuing and distributing digital certificates; and managing and disseminating certificate status information.

According to a PMO official, while the Secretary did not accredit the two processes by October 27, 2005, the Deputy Chief Security Officer accredited DHS' PIV Card Issuer (PCI) service in October 2006. The PMO official said that PCI service accreditation satisfied FIPS 201 PIV-I requirements. While the management and performance of the accreditation activity may be delegated, NIST emphasized that agency heads are required to approve FIPS 201 PIV-I accreditation personally. Further, there exist serious shortcomings in the accreditation of PCI services as reported below.

PCI Services Must Be Re-accredited

DHS did not adequately assess the capabilities and reliability, along with other required and desired attributes, of its PCI services in fulfilling FIPS 201 requirements during the certification and accreditation process. A PCI service

is an authorized PIV Card issuing organization that procures FIPS 201 compliant blank cards, personalizes the cards with the identity credentials of the authorized subjects, and delivers the personalized cards to the authorized applicants. DHS must re-accredit its headquarters PCI services once it has fully developed an operational system with the capability to issue PIV cards.

DHS accredited its headquarters PCI services on October 19, 2006. The certification agent concluded that after assessing the required and desired attributes, the DHS PCI had demonstrated that the DHS PIV issuance system adequately met the intent and content of NIST Special Publication (SP) 800-79.⁷ However, when the PCI services were accredited, DHS did not have an operational system that could produce PIV cards in a production environment, as DHS was still in the process of developing its technical solution, called Identification and Credential Issuing Station and System (ICISS). Furthermore, no stress testing was performed on ICISS to evaluate whether the system had the capabilities to produce PIV cards in large quantities.

In December 2006, after PCI accreditation, the ICISS development team determined that the system could not issue more than five PIV cards before crashing. This situation occurred because DHS accepted the certification agent's accreditation when it lacked a production system capable of producing PIV cards in large quantity.

HSPD-12 specifies that the reliability of a PCI be officially accredited before PIV cards can be issued. NIST requires that the accreditation package document the results of the certification phase and provides the Designated Accreditation Authority with the essential information needed to make a credible, risk-based decision on whether to authorize operation of the PCI. The accreditation package should contain the following documents: (1) Operations Plan, (2) Assessment Report, and (3) Corrective Action Plan. The Operations Plan should further provide supporting material and identity management-related documents, such as the PCI's privacy policy for applicants, and descriptions of procedures for assuring reliable operation.

Obtaining adequate and reliable equipment to support the services provided by the PCI is fundamental to success of its operations. Accreditation of a PCI is the official management decision of the Designated Accreditation Authority to authorize operation of a PCI after determining that the PCI's reliability has

⁷ To assess the reliability of a PCI during the accreditation process, NIST published SP 800-79 with a set of guidelines for federal agencies that issue or prepare to issue FIPS 201 compliant PIV cards to their employees and/or contractors. These guidelines describe a set of attributes that should be exhibited by a PCI in order to be accredited. NIST recommends agencies use these guidelines for assessing the reliability of any organization providing its PCI services.

satisfactorily been established through appropriate assessment and certification processes.

Reliability is the primary attribute to be exhibited and accredited in a PCI and is the characteristic of an organization that requires functions to be performed and services provided as expected, and that this expectation will continue in the future. NIST recommends that a PCI's reliability be evaluated and established by assessing whether the PCI is knowledgeable, capable, accountable, available, legal, compliant, well managed, trustworthy, and adequately supported. If one or more of the required attributes are not present or not expected to continue in the future, then accreditation should be postponed or denied.

Component Implementation Guidance Needs to be Updated

In February 2007, DHS developed a Component Implementation Guidance Package (Guidance Package) to provide instructions for components to implement HSPD-12. The Guidance Package contains DHS' HSPD-12 policy, FIPS 201, *DHS HQ HSPD-12 Procedures Reference Book* (Reference Book), and other NIST special publications. In preparing the package, DHS omitted essential information needed by the components to obtain operational and technical compliance with HSPD-12. For example, the guidance package does not define PIV card specifications, PIV card and middleware conformance testing, and PIV reader specifications.⁸

Furthermore, while the Reference Book contains detailed instructions on issuing PIV cards to new employees and contractors, it does not contain procedures relating to current employees and contractors. We also identified the following deficiencies in the Reference Book that DHS must revise to ensure the successful implementation of HSPD-12:

- The timeframe for a PIV cardholder to notify a supervisor and security officer of a lost, stolen, or compromised PIV card contradicts with a FIPS 201 requirement. The Reference Book requires PIV cardholders to report lost, stolen, or compromised PIV card within 24 hours. FIPS 201 requires PIV cardholders to report lost, stolen, or compromised PIV card within 18 hours.
- The length of personal identification numbers (PIN) and emergency notification procedures to inform supervisors and security in the event of

⁸ SP 800-73-1, *Interfaces for Personal Identity Verifications*, March 2006; SP 800-76-1, *Biometric Data Specification for Personal Identification Verification*, January 2007, and SP 800-78, *Cryptographic Algorithms and Key Sizes for Personal Identity Verification*, April 2005; SP 800-85A, *PIV Card Application and Middleware Interface Test Guidelines (SP 800-73 compliance)*, April 2006, SP 800-85B, *PIV Data Model Conformance Test Guidelines*, July 2006, and SP 800-96, *PIV Card/Reader Interoperability Guidelines*, September 2006.

lost, damaged, and compromised PIV cards have not been established. The Reference Book only advises applicants to choose a PIN carefully but does not specify the length of the PIN, and does not contain emergency notification procedures.

- Separation of duties needs to be established to ensure that one person cannot issue a PIV card to a person not entitled to the card or issue a card with incorrect information. The Reference Book allows the same person to fill the Access Control Officer specialist, enrollment officer, and PIV issuer roles. FIPS 201 requires that the roles of PIV Applicant, Sponsor, Registrar, and Issuer are mutually exclusive and that no individual shall hold more than one of these roles in the identity proofing and registration process.
- Account lockout does not meet DHS requirements. The Reference Book allows cardholders ten attempts to gain logical access with their PIV card and PIN before the card is locked out. *DHS 4300A Sensitive Systems Handbook* requires that the user account should be locked out after three failed login attempts.

Without adequate guidance from the PMO, there is little assurance that the implementation of HSPD-12 across the department will be successful and effective in securing DHS facilities and information systems.

PIV Card Issuance Statistics Not Posted On Public Website

OMB requires federal agencies to post on their public websites, beginning March 1, 2007, a quarterly status report on the total number of employees requiring PIV cards, and the number of PIV cards that have been issued to their employees, contractors, and visitors. OMB established this requirement in order to monitor agencies' progress in implementing HSPD-12.⁹

Citing operational security concerns associated with posting such information on its public website, DHS drafted a letter to OMB listing its reasons not to comply with this requirement. As cited in DHS' letter, revealing the total number of employees requiring PIV cards poses security vulnerability when compared against the total number of PIV cards issued. Furthermore, according to DHS, the public release of this information could reveal DHS' HSPD-12 readiness and may result in data mining by individuals attempting to identify employees at agencies that are not compliant, or have not fully implemented HSPD-12 requirements. However, other federal agencies have posted this information to their websites, including the Agriculture Department, Commerce Department, Defense Department, Energy

⁹ OMB M-07-06, *Validating and Monitoring Agency Issuance of Personal Identity Verification Credentials*, dated January 11, 2007.

Department, Justice Department, State Department, Transportation Department, Treasury Department, and Veterans Affairs Department. OMB's Deputy General Counsel said that DHS has not formally voiced any concerns for not complying with this reporting requirement.

DHS Is Not Ready to Issue HSPD-12 Compliant Cards

DHS does not have a certified and accredited operational system to support the implementation of HSPD-12. Specifically, DHS has not acquired the capability to issue PIV cards to its headquarters employees and contractors, and bring its system to production readiness.

PMO Needs to Bring Headquarters System to Production Readiness

DHS does not have a production system having the capability to support the implementation of HSPD-12 by issuing PIV cards to its employees and contractors. Without a viable system, DHS cannot meet OMB's milestones and ultimately improve physical and logical security at its facilities and for its information systems.

In June 2006, DHS tasked a contractor to upgrade and enhance the ICISS, develop interfaces to existing HSPD-12 preproduction systems, and perform work to certify and accredit ICISS. During a functional test in December 2006, DHS determined that ICISS could not perform all of the system requirements and could not interface with other existing external and internal DHS systems. In addition, the system crashed after producing five PIV cards. No stress testing had been performed to determine the system's capacity and whether ICISS would be able to support DHS' workload. Furthermore, ICISS could not accept all identity documents that are listed in OMB Form I-9, which DHS accepts as evidence to verify applicants' identities. See Appendix D for a list of OMB acceptable documents.

Due to the technical issues identified with ICISS, DHS officials are in the process of issuing a new contract. The new contract will task the contractor to deliver a new technical solution that will provide an end-to-end PIV solution, including required interfaces. According to the PMO's April 20, 2007 implementation schedule, the headquarters system would be production ready by July 2007 and will begin issuing PIV cards to new headquarters employees and contractors by December 2007. As of July 2007, no contract had been let. Nonetheless, DHS officials expect to have a new technical solution operational by the end of 2007, 6 months behind its implementation schedule.

Certification of ICISS Was Inadequate and Not Independent

The certification of ICISS was inadequately performed and the certification agent was not independent of the development team. The goal established by DHS was to have ICISS certified and accredited by September 30, 2006.

The contractor who developed ICISS was requested, as certification agent, to conduct security testing to evaluate the effectiveness of controls implemented. The certification agent is an individual, group, or organization responsible for conducting a security certification, or comprehensive assessment of the controls implemented on an information system to determine whether the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. The certification agent also provides recommended corrective actions to reduce or eliminate vulnerabilities in the information system. Furthermore, prior to initiating the security assessment activities that are a part of the certification process, the certification agent also provides an independent assessment of the system security plan to ensure the plan provides a set of security controls for the information system that is adequate to meet all applicable security requirements.

The effectiveness of the controls implemented on ICISS and other interconnected systems was not evaluated in a production environment. Security testing was performed only in the test environment. In addition, the contractor was tasked to prepare security documents, such as the system security plan, risk assessment, and system test and evaluation plan, to support the accreditation decision. When ICISS was accredited with an authority to operate for a period of 1 year, on October 20, 2006, the system was still in development and interfaces with other systems that are required to perform fingerprint checks and control PIV cardholders' access to facilities had not been established.

The information and supporting evidence needed for security accreditation is developed during a detailed security review of an information system, typically referred to as security certification. Security certification is a comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

Security accreditation is the official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations, agency assets, or individuals based on the implementation of an agreed-upon set of security controls. By

accrediting an information system, an agency official accepts responsibility for the security of the system and is fully accountable for any adverse impacts to the agency if a breach of security occurs. Without an independent and thorough assessment of the system, the accreditation official was not provided with the most complete, accurate, and trustworthy information possible. The security status of the information system is needed in order to make timely, credible, risk-based decisions on whether to authorize operation of the system.

To preserve the impartial and unbiased nature of the security certification, the certification agent should be independent from the persons directly responsible for the development of the information system and the day-to-day operation of the system. NIST recommends that the certification agent be independent of those individuals responsible for correcting security deficiencies identified during the security certification. When the potential agency-level impact of the system is moderate or high, certification agent independence is needed and justified.

Recommendations

We recommend that the Under Secretary for Management direct the DHS HSPD-12 PMO to:

Recommendation #1: Evaluate DHS' implementation plan and take necessary steps to include the identification of additional resources to ensure that milestones are met or exceeded and that further delays are avoided.

Recommendation #2: Develop a department-wide cost estimate to ensure the determination of the most cost effective technical solution and also ensure that sufficient resources are allocated to implement HSPD-12.

Recommendation #3: Work with all DHS components to identify the facilities access points and information systems where the PIV cards will be required.

Recommendation #4: Ensure that the agency head accredits the PIV-I processes. In addition, the DHS PMO should re-accredit the headquarters PCI services after the PIV system becomes operational and supporting documentation is revised to include all required information.

Recommendation #5: Revise component guidance to include procedures for issuing PIV cards, including adequate separation of duties, in compliance with FIPS 201 and DHS requirements.

Recommendation #6: Perform the certification and accreditation of the information systems used to implement HSPD-12 and FIPS 201 in accordance

with applicable NIST and DHS guidance. In addition, the HSPD-12 PMO should provide agency officials with the most accurate information to make credible, risk-based decisions on whether to authorize a system to operate.

Recommendation #7: Ensure that OMB reporting statistics are posted on DHS' website.

Management Comments and OIG Analysis

We obtained written comments on a draft of this report from the Under Secretary for Management. Generally, the Under Secretary agreed with the report's findings and recommendations. Where appropriate, we made changes to the body of the report to address the Under Secretary's comments. We have included a copy of the comments in its entirety as Appendix B.

DHS concurred with recommendation 1. The PMO continues to evaluate its implementation plan to promote a balanced approach for resource allocation. On August 2, 2007, a request for contract proposal was issued to procure an identity management system and credentialing issuance and maintenance support. When the contract is awarded, it will provide a means to deploy a unified system across the department for issuing a secure and tamper-proof smart card that allows interoperable access to DHS facilities and information systems.

We agree that the steps the PMO is taking, and plans to take, begin to satisfy this recommendation. However, the PMO did not fully address our recommendation to evaluate its implementation plan to ensure that milestones are met and future delays are avoided.

DHS concurred with recommendation 2. In May 2007, the PMO completed an independent government cost estimate, as a baseline, to evaluate the cost of implementing HSPD-12 throughout the department. However, each component has the responsibility for identifying and budgeting resources to implement its HSPD-12 efforts. The PMO will continue to work with the components to develop a proper budget estimate to implement HSPD-12.

We agree that the steps the PMO has taken, and plans to take, satisfy this recommendation.

DHS concurred with recommendation 3. The PMO has requested that the components identify their current and future requirements for facilities, physical and logical access controls, and provide this information to the PMO.

We agree that the steps the PMO plans to take satisfy this recommendation.

DHS concurred with recommendation 4. Once the new technical solution is in place, the PMO will re-certify and accredit DHS' PCI service to ensure that there is complete integration between the operational procedures and the technical capability, and DHS remains in compliance with FIPS 201 and other applicable NIST special publications. However, the PMO continues to maintain that when the Deputy Chief Security Officer accredited DHS' PCI service in October 2006, it satisfied FIPS 201 PIV-I requirements.

We agree that the steps the PMO plans to take begin to satisfy this recommendation. However, we maintain that the agency head should accredit the PIV-I processes. FIPS 201, which is compulsory and binding for federal agencies, requires agency heads to accredit the processes personally.

DHS concurred with recommendation 5. The PMO has established the required separation of duties in the Reference Book.

We agree that the steps the PMO has taken begin to satisfy this recommendation. However, the PMO did not fully address our recommendation to include procedures in the Reference Book on issuing PIV cards to current employees and contractors, notifying supervisor and security office within 18 hours in the event of a lost, stolen, or compromised PIV card, specifying the length of PIN, and ensuring that account lockout comply with DHS policy.

DHS concurred with recommendation 6. The PMO plans to obtain a new certification and accreditation of the information system used to support HSPD-12 at DHS headquarters, as part of the process to implement a new technical solution.

We agree that the steps DHS plans to take satisfy this recommendation.

DHS did not concur with recommendation 7. The Chief Security Officer determined that revealing the total number of employees requiring and carrying PIV cards is not in the best interest of national security. However, the PMO will provide these statistics to OMB using a method other than a public website.

We maintain that DHS should comply with OMB reporting instructions and post its HSPD-12 issuance statistics on its website.

Appendix A

Purpose, Scope, and Methodology

Our objective was to determine whether DHS has effectively managed the implementation of HSPD-12. We determined whether DHS': (1) HSPD-12 implementation strategy plan is adequate; (2) policies and procedures to implement HSPD-12 requirements are adequate; and (3) security controls implemented to protect the privacy of personal data collected and processed by HSPD-12 systems are effective.

To accomplish our audit, we interviewed selected DHS personnel responsible for implementing HSPD-12 requirements. We reviewed the implementation plan, policies, and procedures developed to implement HSPD-12 requirements for compliance with applicable OMB and NIST guidance. We also reviewed selected security documents to evaluate whether security controls were implemented on ICISS to protect the privacy of personal data. In addition, we contacted OMB officials to obtain clarifications on their implementation instructions and feedback on DHS submissions.

We did not evaluate DHS' identity proofing and registration process and PIV card issuance and maintenance process since the department is not issuing PIV cards. In addition, since the department has not implemented a system to produce PIV cards, we could not determine if security controls have been adequately implemented to protect the privacy of personal data collected and processed.

We conducted our audit between April 2007 and June 2007 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 E.

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.


Appendix B
Management Comments to the Draft Report

Under Secretary for Management
U.S. Department of Homeland Security
Washington, DC 20528



SEP 20 2007

MEMORANDUM FOR: Frank W. Deffer
Assistant Inspector General, IT Audits

FROM: Paul A. Schneider
Under Secretary for Management 

SUBJECT: Response to Department of Homeland Security, Office of Inspector
General Draft Report titled: *"Progress Has Been Made But More Work
Remains in Meeting HSPD-12 Requirements,"* dated August 2007

Thank you for providing the Department of Homeland Security (DHS) the opportunity to review and comment on the Office of Inspector General (OIG) draft report *"Progress Has Been Made But More Work Remains in Meeting HSPD-12 Requirements,"* dated August 2007.

On August 27, 2004, the President signed Homeland Security Presidential Directive – 12 (HSPD-12) titled *"Policy for a Common Identification Standard for Federal Employees and Contractors."* The Directive requires the development and agency implementation of a mandatory, government-wide standard for secure and reliable forms of identification for Federal employees and contractors. The DHS OIG initiated an audit to determine whether the Department's HSPD-12 implementation plan has:

- the necessary policies and procedures in place to implement HSPD-12 requirements; and,
- effective security controls to protect the privacy of personal data collected and processed by HSPD-12 systems.

The OIG made seven recommendations for the HSPD-12 Program Management Office (PMO) to implement. Management would like to take this opportunity to address the following recommendations contained in the report.

1. The Background Section of the OIG draft report states that, "The DHS Office of Security is responsible for all aspects of the Department's HSPD-12 implementation."

Although the Office of Security is responsible for the implementation of HSPD-12, the Office of the Chief Information Officer (OCIO) is responsible for the technical aspects of the program. The OCIO provides the program with valuable expertise in defining technical requirements and evaluating proposed solutions, while the PMO provides policy, procedure, and program management guidance and facilitates collaboration among the components. Throughout the course of the HSPD-12 implementation, the Office of Security PMO and OCIO have collaborated to provide the most

Appendix B Management Comments to the Draft Report

effective programmatic and technical solution for the DHS HSPD-12 compliant credential.

OIG: Revised.

2. The report contains the statements that “DHS Is Behind In Its Implementation Schedule and Will Not Meet OMB Milestones” and that “Federal agencies are required to phase in the issuance and use of Personal Identity Verification (PIV) cards for all new employees and contractors by October 27, 2007, and complete the issuance of PIV cards to all employees by October 27, 2008. DHS is not scheduled to complete its HSPD-12 implementation until 2010, which is two years after OMB’s mandated deadline.”

This ignores the fact that DHS, through the HSPD-12 PMO, has received approval for a PIV-II full compliance deadline of Fiscal Year (FY) 2010. Although the deadline for DHS to issue credentials to all employees and contractors has been extended to 2010, the Office of Management and Budget (OMB) did request that DHS make significant progress by December 2008 and issue credentials to the majority of its workforce. In working to achieve this goal, the Office of Security developed an agency-wide implementation plan, which has been approved by OMB. As the implementation progresses, the DHS HSPD-12 PMO, working with the components, provides regular updates to OMB on the status and schedule of the Department’s HSPD-12 activities. DHS will continue to work collaboratively with OMB to ensure compliance with the OMB-approved implementation schedule.

OIG: Changed statement from “Will Not” to “May Not”; added response from OMB.

3. The audit report also states that DHS has completed only one of four tasks associated with completing Phase I of this effort.

This is an inaccurate statement. We have completed a thorough cost assessment, which included an Independent Government Cost Estimate (IGCE) of the HSPD-12 program at DHS as opposed to using the General Services Administration’s (GSA) Managed Service Offering (MSO). The inference that DHS has not yet begun PIV issuance is incorrect. DHS issued a compliant PIV card on October 19, 2006. Card issuance continued for three months under limited rate production, due to system constraints, before production was ceased in favor of seeking a more robust technical solution.

DHS determined not to utilize the GSA solution for functional, operational, and financial reasons. Based on the IGCE, DHS will save more than \$20 million by managing its own PIV solution. This is based on a three-year cost of \$174.25 per card, if acquired via GSA versus approximately \$60.00 per card if DHS continues with its current plan; multiplying the difference of \$114.25 per card by approximately 210,000 employees at the Department yields an initial outlay saving of almost \$24 million.

Furthermore, from an operational perspective, by developing an HSPD-12 solution, DHS is able to:

- issue HSPD-12 compliant credentials containing four public key infrastructure certificates and two fingerprint templates;
- maintain a secure backend cardholder and card management system; and
- implement a nationwide network of fixed and mobile enrollment stations shared by all components of DHS.

The Department is able to more easily control credential usage, as it does not have to rely on a third party to integrate its physical access control systems.

Appendix B Management Comments to the Draft Report

From a security perspective, by utilizing GSA's MSO, DHS is entrusting sensitive information regarding employees to a third party to manage – information that will likely include employees operating in critical roles.

OIG: During fieldwork we were told by a PMO official that only 8 cards were issued before ceasing production, and that no cost estimates were developed prior to deciding not to use GSA.

4. The report asserts that “Agency Head Has Not Accredited PIV-I Process.”

DHS received PIV-II accreditation at DHS HQ on October 19, 2006, and was granted Authority to Operate (ATO). The accreditation of PIV-II is a de-facto accreditation of the PIV-I processes, and includes the review of both PIV-I and PIV-II procedures, controls, and technologies utilized by the credential-issuing organization.

In 2005, DHS implemented an approved PIV-I process. The Department adopted the National Institute of Standards and Technology (NIST) Model for PIV-I credential issuance and maintenance. In accordance with FIPS 201-1, DHS completed FIPS 201-1 Part 1 requirements for “identification issued based on sound criteria for verifying an individual’s identity.” The completed tasks included the approved credential issuance maintenance process, as defined by FIPS 201 section 2.0.

The current NIST policy does not require that an agency head personally accredit PIV Card Issuer (PCI) PIV-II processes. NIST guidance requires that a Designated Accreditation Authority (DAA), who is a federal employee and a senior agency official, accredit PCIs following an official accreditation process. The DHS Deputy Chief Security Officer (DCSO) served as the DAA and, in consultation with the DHS Chief Security Officer (CSO), directed departmental components to designate personnel to fulfill the roles and responsibilities required to implement the compliant PIV-I credentialing model.

Based on the NIST recommended process, the DHS DAA, Jerry Williams, reviewed the certification and accreditation (C&A) package, including the recommendation prepared by the certification agent (CA), and made an accreditation determination. Mr. Williams then provided the DHS HQ PCI with ATO on October 19, 2006.

OIG: We maintain that the agency head should accredit the PIV-I processes. NIST stated in FIPS 201, which is compulsory and binding for federal agencies, that agency heads are required to accredit processes personally.

5. The draft audit also states the following: “DHS did not adequately assess the capabilities and reliability, along with other required and desired attributes, of its PCI services in fulfilling FIPS 201 requirements during the C&A process. A PCI service is an authorized PIV Card issuing organization that procures FIPS 201 compliant blank cards, personalizes the cards with the identity credentials of the authorized subjects, and delivers the personalized cards to the authorized applicants. DHS must re-accredit its headquarters’ PCI services once it has fully developed an operational system with the capability to issue PIV cards.”

In fact, DHS accredited its headquarters PCI services on October 19, 2006. After assessing the required and desired attributes, the certification agent concluded the DHS PCI had demonstrated that the DHS PIV issuance systems adequately met the intent and content of NIST Special Publication (SP) 800-79.8. This system, called Identification and Credential Issuing Station and System (ICISS), could not be placed in the production environment until the PCI services were accredited. Therefore, no stress testing could be conducted at that time to evaluate whether the system had the capability to produce PIV cards in large quantities. Once ICISS was on the DHS network and testing was completed, DHS determined that a more robust technology needed to be developed. DHS has issued a

Appendix B Management Comments to the Draft Report

Blanket Purchase Agreement (BPA), which solicits the services of experienced PIV vendors, to provide production services. When the new production system has been implemented, it will be re-accredited.

OIG: The issue is not that the PCI service was not accredited, only that it should not have been due to issues explained in the report.

6. The report also states that, “In December 2006, after PCI accreditation, the ICISS development team determined that the system could not issue more than five PIV cards before crashing. This situation occurred because DHS accepted the certification agent’s accreditation when it lacked a production system capable of producing PIV cards in large quantity. In addition, the PCI Operations Plan did not contain the privacy policy and detail procedures to enroll and issue PIV cards to current employees and contractors.”

Accreditation of a PCI is the official management decision of the DAA to authorize operation of a PCI after determining that the PCI’s reliability has satisfactorily been established through appropriate assessment and certification processes.

As stated earlier, with the approval of the DAA, the system was certified and accredited on October 19, 2006. Since the system could not be placed in a production environment prior to completion of C&A, there was no means to test the scalability of the system on the DHS network prior to the October 19 date. As noted, the issue of system scalability was recognized in December and was addressed by the OCIO and HSPD-12 PMO’s efforts to acquire a new technical solution. Once in place, this new solution will also be re-certified and re-accredited and tested for scalability on the DHS network.

The privacy of the applicant is addressed in the DHS HSPD-12 Personal Identity Verification Privacy Impact Assessment, dated October 13, 2006, and published on the DHS Privacy website, which deems that the procedures outlined in the DHS HSPD-12 Reference Book properly protect the privacy of the applicants. The PCI Operations Plan requires the PCI to ensure that all managers and staff understand these procedures and that they follow all document storage and privacy information protection procedures therein.

OIG: Deleted last sentence.

7. The DHS IG report states that, “Component Implementation Guidance Needs to be Updated” and that inadequacies exist in the Guidance Packages provided to the components.

The Guidance Package was developed to help component HSPD-12 project teams in their implementation of the directive. The decision to change direction with regard to the technical solution prevented the inclusion of information on that aspect of the project. Placeholders were inserted so, once available, that information could be added to any Guidance Packages.

The current Package includes detailed descriptions of the operational requirements for HSPD-12 in their entirety, including PIV Card specification (DHS HSPD-12 Requirements for All DHS Personnel), and procedures for testing individual cards (Reference Book – Section 3.4 Issuance). The report also claims that there is no plan to issue PIV cards to existing employees but, as noted in the Implementation Plan submitted to OMB, the PMO will address this requirement as part of Phase III.

Finally, Management concurs with six of the seven recommendations contained in the OIG draft report. In each of these instances, the recommendation is part of Office of the Chief Security Officer

Appendix B Management Comments to the Draft Report

(OCSO) established policy for the HSPD-12 program; implementation actions have either been completed, or will be completed, as part of the enterprise DHS solution presently under procurement. Management's responses to the seven recommendations are as follows:

Recommendation #1: Evaluate DHS' implementation plan and take necessary steps to include the identification of additional resources to ensure that milestones are met or exceeded and that further delays are avoided.

Management Concur: The HSPD-12 PMO continually evaluates its implementation plan to promote a balanced approach to resource allocation. Procurement of an enterprise-wide HSPD-12 technical solution began on August 2, 2007, when a Request for Proposal (RFP) to establish a departmental BPA for an Identity Management System and credentialing issuance and maintenance support, was released. When this contract is awarded, it will provide a means to deploy a unified system across the Department for a secure, tamper-proof smart card that allows interoperable access to DHS facilities and systems.

Recommendation #2: Develop a Department-wide cost estimate to ensure the determination of the most cost effective technical solution and also ensure that sufficient resources are allocated to implement HSPD-12.

Management Concur: The DHS HSPD-12 PMO completed an IGCE for the HSPD-12 Program in May 2007. The PMO estimate evaluated HSPD-12 implementation costs across the Department. This IGCE, however, can only be used as a baseline for evaluation, as each component has the responsibility for budgeting for HSPD-12 and identifying resources to support this effort. The DHS HSPD-12 PMO will continue to work with the components to promote proper forecasting and budgeting for this program.

Recommendation #3: Work with all DHS components to identify the facilities' access points and information systems where the PIV cards will be required.

Management Concur: The DHS HSPD-12 PMO has requested information on both the current and future requirements for facilities, physical and logical access control from DHS components. The PMO is actively involved in gathering the required information using the PMO's Data Input and Monitoring Dashboard (DIAMonD) data collection tool.

Recommendation #4: Ensure that the agency head accredits the PIV-I processes. In addition, the DHS PMO should re-accredit the headquarters' PCI services after the PIV system becomes operational and supporting documentation is revised to include all required information.

Management Concur: DHS received PIV-II accreditation at DHS Headquarters on October 19, 2006, and was granted ATO. The accreditation of PIV-II is a de-facto accreditation of the PIV-I process, and includes the review of both PIV-I and PIV-II procedures, controls, and technologies utilized by the credential-issuing organization. As the requirements for C&A of PIV-II were released

Appendix B Management Comments to the Draft Report

without the requirement for an "agency head" but rather a "Senior Agency Official" (See NIST SP 800-79), the PMO recognizes the Deputy Chief Security Officer's approval of the C&A on PCI Services in October 2006 as the appropriate approval for PIV-I functions. During the October 2006 C&A, all policies, procedures, and roles pertaining to PIV- and PIV-II were addressed.

Once the technical solution is in place, the DHS HSPD-12 PMO will re-certify and re-accredit the HSPD-12 Policies and Procedures to ensure that:

- there is a complete integration between the operational procedures and the technological capability; and,
- DHS remains in compliance with the requirements of FIPS 201, SP 800-79 or other related NIST publications.

Recommendation #5: Revise component guidance to include procedures for issuing PIV cards, including adequate separation of duties, in compliance with FIPS 201 and DHS requirements.

Management Concur: The DHS HSPD-12 PMO has established the required separation of duties in the DHS HSPD-12 Reference Book. This position is supported by Section A.1.1.1 of FIPS 201, which states the following: "The roles of PIV Applicant, Sponsor, Registrar, and Issuer are mutually exclusive; no individual shall hold more than one of these roles in the identity proofing and registration process." The roles of Enrollment Official and PIV Issuer are, however, not mutually exclusive. The DHS-specific role of Access Control Office specialist may also perform both of these non-exclusive roles.

Recommendation #6: Perform the certification and accreditation of the information systems used to implement HSPD-12 and FIPS 201 in accordance with applicable NIST and DHS guidance. In addition, the HSPD-12 PMO should provide agency officials with the most accurate information to make credible, risk-based decisions on whether to authorize a system to operate.

Management Concur: The HSPD-12 PMO plans to obtain a new C&A of the information system used to support HSPD-12 at DHS Headquarters as part of the process to implement a new technical solution, following award of task order one of the BPA.

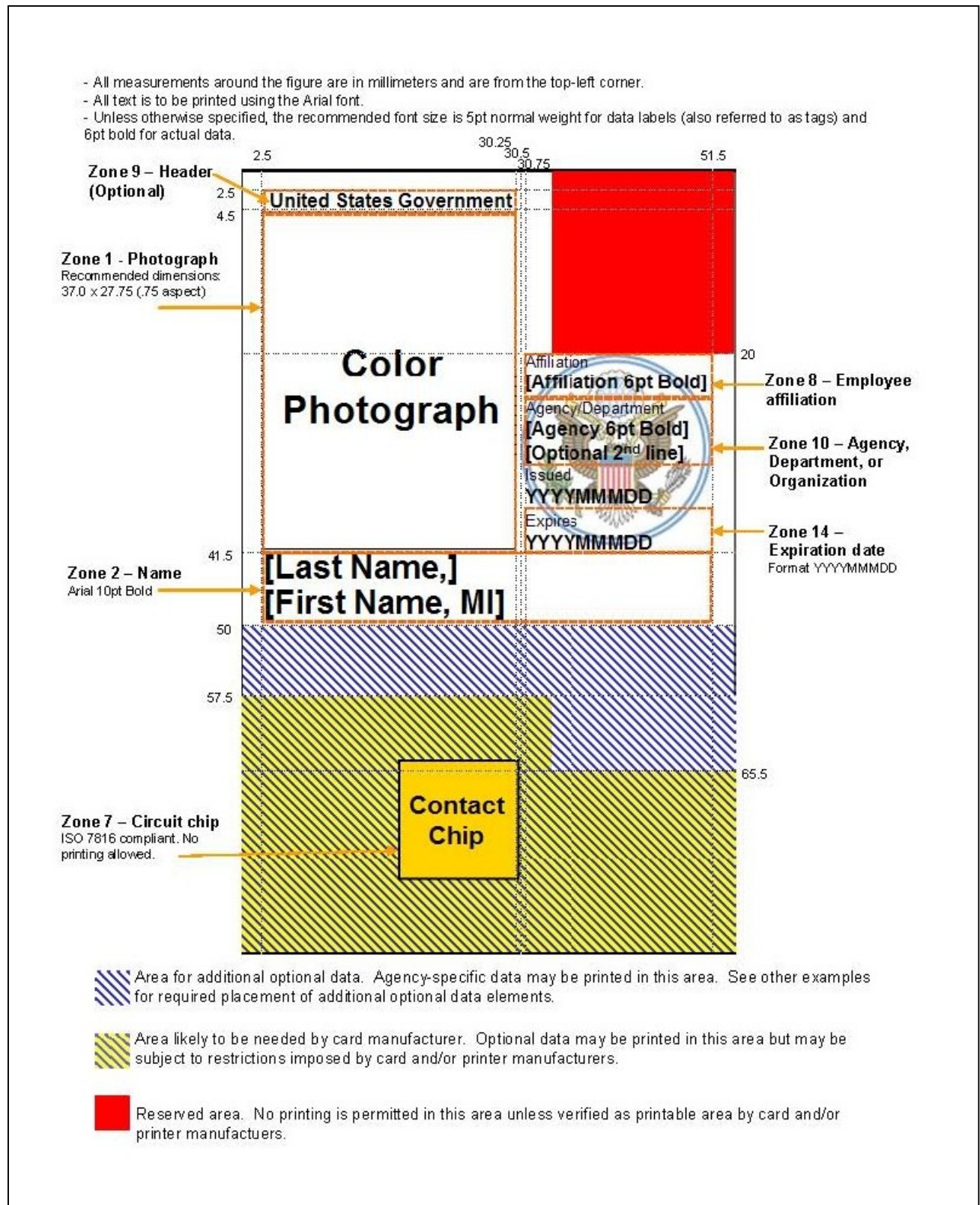
Recommendation #7: Ensure that OMB reporting statistics are posted on DHS' Website.

Management Non-Concur: OMB has put forth a requirement that agencies post their reporting statistics on public websites. DHS Management does not concur with the recommendation. The CSO has determined that revealing the total number of employees requiring and carrying DHS PIV cards is not in the best interest of national security.

The public release of this information could reveal the Department's HSPD-12 readiness and may result in data mining by individuals attempting to identify employees. However, the HSPD-12 PMO will work to provide these statistics to OMB, using a method other than a public Website.

Appendix C

Example of a PIV card



Appendix D
OMB Form I-9 Lists of Acceptable Documents

LISTS OF ACCEPTABLE DOCUMENTS

LIST A	OR	LIST B	AND	LIST C
Documents that Establish Both Identity and Employment Eligibility		Documents that Establish Identity		Documents that Establish Employment Eligibility
<ol style="list-style-type: none"> 1. U.S. Passport (unexpired or expired) 2. Certificate of U.S. Citizenship (Form N-560 or N-561) 3. Certificate of Naturalization (Form N-550 or N-570) 4. Unexpired foreign passport, with I-551 stamp or attached Form I-94 indicating unexpired employment authorization 5. Permanent Resident Card or Alien Registration Receipt Card with photograph (Form I-151 or I-551) 6. Unexpired Temporary Resident Card (Form I-688) 7. Unexpired Employment Authorization Card (Form I-688A) 8. Unexpired Reentry Permit (Form I-327) 9. Unexpired Refugee Travel Document (Form I-571) 10. Unexpired Employment Authorization Document issued by DHS that contains a photograph (Form I-688B) 	OR	<ol style="list-style-type: none"> 1. Driver's license or ID card issued by a state or outlying possession of the United States provided it contains a photograph or information such as name, date of birth, gender, height, eye color and address 2. ID card issued by federal, state or local government agencies or entities, provided it contains a photograph or information such as name, date of birth, gender, height, eye color and address 3. School ID card with a photograph 4. Voter's registration card 5. U.S. Military card or draft record 6. Military dependent's ID card 7. U.S. Coast Guard Merchant Mariner Card 8. Native American tribal document 9. Driver's license issued by a Canadian government authority <p>For persons under age 18 who are unable to present a document listed above:</p> <ol style="list-style-type: none"> 10. School record or report card 11. Clinic, doctor or hospital record 12. Day-care or nursery school record 	AND	<ol style="list-style-type: none"> 1. U.S. social security card issued by the Social Security Administration (other than a card stating it is not valid for employment) 2. Certification of Birth Abroad issued by the Department of State (Form FS-545 or Form DS-1350) 3. Original or certified copy of a birth certificate issued by a state, county, municipal authority or outlying possession of the United States bearing an official seal 4. Native American tribal document 5. U.S. Citizen ID Card (Form I-197) 6. ID Card for use of Resident Citizen in the United States (Form I-179) 7. Unexpired employment authorization document issued by DHS (other than those listed under List A)

Appendix E
Major Contributors to this Report

Information Security Audits Division

Edward G. Coleman, Director

Jeff Arman, Audit Manager

Chiu-Tong Tsang, Audit Team Leader

Charles Twitty, Auditor

Steven Staats, Referencer

Appendix F

Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy Chief of Staff
General Counsel
Executive Secretary
Assistant Secretary for Policy
Assistant Secretary for Public Affairs
Assistant Secretary for Legislative Affairs
Under Secretary for Management
Chief Security Officer
Chief Information Officer
Deputy Chief Information Officer
Chief Information Security Officer
Director, Compliance and Oversight Program
Director, DHS HSPD-12 Program Management Office
Director, DHS GAO/OIG Liaison Office
Chief Information Officer Audit Liaison
Director, 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, call the Office of Inspector General (OIG) at (202) 254-4199, 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.