Privacy Impact Assessment
for the

Personal Identity Verification

October 13, 2006

Contact Point

Cynthia Sjoberg
Program Manager, HSPD-12
Training and Operations Security Division
Office of Security
Department of Homeland Security
(202) 447-5010

Reviewing Official

Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security
(571) 227-3813

Introduction

Program Overview

Homeland Security Presidential Directive 12 (HSPD-12), issued on August 27, 2004, required the establishment of a standard for identification of Federal Government employees and contractors. HSPD-12 directs the use of a common identification credential for both logical and physical access to federally controlled facilities and information systems. This initiative is intended to enhance security, increase efficiency, reduce identity fraud, and protect personal privacy.

HSPD-12 requires that the Federal credential be secure and reliable. A secure and reliable credential is defined by the Department of Commerce (DOC) as a credential that:

- Is issued based on sound criteria for verifying an individual's identity
- Is strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation
- Can be rapidly authenticated electronically
- Is issued only by providers whose reliability has been established by an official accreditation process

The National Institute of Standards and Technology (NIST) was asked to produce a standard for secure and reliable forms of identification. In response, NIST published Federal Information Processing Standard Publication 201 (FIPS 201), Personal Identity Verification (PIV) of Federal Employees and Contractors, issued on February 25, 2005. The credential is for physical and logical access, and other applications as determined by the individual agencies.

FIPS 201 consists of two parts: PIV I and PIV II. The standards in PIV I support the control objectives and security requirements described in FIPS 201, including the standard background investigation required for all Federal employees and long-term contractors. The standards in PIV II support the technical interoperability requirements described in HSPD-12. PIV II also specifies standards for implementing identity credentials on integrated circuit cards (i.e., smart cards) for use in a Federal PIV system. Simply stated, FIPS 201 requires agencies to:

- Establish new roles to facilitate identity proofing, information capture and storage, card issuance and maintenance, and privacy concerns.
- Develop and implement a new physical and technical infrastructure.
- Establish processes to support the implementation of a PIV program.

In response to HSPD-12 and to meet the requirements summarized above, the Department of Homeland Security's (DHS) Office of Security is responsible for the identity management and all aspects of the Department's HSPD-12 implementation including serving as the main internal and external point of contact with respect to program planning, operations, business management, communications and technical strategy. The Department is currently expecting to equip approximately 5500 PIV cards for physical and logical access at two facilities nationwide beginning in fiscal year 2007.

PIA Scope

This PIA provides detail about DHS's role in the collection and management of personally identifiable information (PII) for the purpose of issuing credentials (ID badges) to meet the requirements of HSPD-12 and comply with the standards outlined in FIPS 201 and its accompanying special publications. HSPD-12 requires a standardized and secure process for personal identity verification through the use of advanced and interoperable technology. This resulted in a need to collect biographic and biometric information. This PIA covers the information collected, used, and maintained for these processes, specifically the: (i) background investigation; (ii) identity proofing and registration; (iii) Identity Management System (IDMS), the database used for identity management and access control; and (iv) the PIV card.

As noted previously, PIV-I requires the implementation of registration, identity proofing, and issuance procedures in line with the standards of FIPS 201; however, the collection of information for background investigations has been a long-standing requirement for Federal employment. This process and the elements used are not new. The forms and information collection for the background investigation process will continue to occur. The PIV-I does not require the implementation of any new systems or technology. The DHS will continue to issue existing ID badges under PIV-I, but the process for credential application and issuance will conform to requirements of HSPD-12 and FIPS 201.

This PIA covers both the PIV-I and PIV-II processes. This system will be referred to throughout this PIA as the DHS's PIV system and the credentials issued referred to as PIV cards.

Basic Program Control Elements

Secure and reliable forms of identification for purposes of this directive means identification that (a) are issued based on sound criteria for verifying an individual employee's identity; (b) are strongly resistant to identify fraud, tampering, counterfeiting, and terrorist exploitation: (c) can be rapidly authenticated electronically; and (d) are issued only by providers whose reliability has been established by an official accreditation process.

Each agency's PIV implementation must meet the above four control objects such that:

- Credentials are only issued (1) to individuals whose true identity has been verified, and (2) after a proper authority has authorized issuance of the credential.
- Only an individual with a completed background investigation on record is issued a credential.
- An individual is issued a credential only after presenting two-identity source documents, at least one of which is a valid Federal or state government picture identification document.
- Fraudulent or altered identity source documents are not accepted as genuine.
- A person suspected or known to the government as a terrorist is not issued a credential.

No substitution occurs in the identity-proofing process. More specifically, the individual who appears for identity proofing, and whose fingerprints are checked, is the person to whom the credential is issued. This means:

- No credential is issued unless requested by proper authority
- A credential remains serviceable only up to its expiration date. A revocation process exists such

that expired or invalidated credentials are swiftly revoked.

- A single corrupt official in the process cannot issue a credential with an incorrect identity or to a person not entitled to the credential.
- An issued credential is verified to not be modified, duplicated, or forged.

As a basic data flow, DHS collects fingerprints and background check paperwork from applicants. DHS submits each set of information to OPM. OPM then submits the fingerprint card to the FBI in order to conduct the fingerprint checks. The FBI provides the results (no match or match with criminal record reference) of the check to OPM who then provides them to DHS along with their own background check results. Once DHS receives the results of the background check a Personnel Security Assistant, the individual validating the receipt of the background check, authorizes the issuance of a credential in the vetting database Personnel Security Activities Management System (PSAMS)[1]. The authorization and the required data to proceed with the card issuance process is transferred to the PIV Identity Management System (IDMS) which manages the issuance of the PIV credential. The enrollment officer then reviews the personnel profile and issues the card to the employee or contractor. Any information regarding the background investigation is retained in PSAMS, not in IDMS or on the PIV card itself.

The Office of the Chief Information Officer(OCIO) is actively working to use the connectivity between US-VISIT's IDENT system and Department of Justices FBI's system to send the fingerprints directly to the Department of Justice/FBI. Department of Justice/FBI would then provide the results as indicated back to DHS. It is anticipated that this connectivity will be in place by December 2006.

Section One: Information Collected and Used in the PIV Program

1.1 What information is collected and from whom?

The PIV Applicant may be a current or prospective Federal hire, a Federal employee or a contractor. As required by FIPS 201, DHS will collect biographic and biometric information from the PIV Applicant in order to: (i) conduct the PIV background investigation; (ii) complete the identity proofing and registration process; (iii) create a data record in the PIV Identity Management System (IDMS); and (iv) issue a PIV card. Figure 1 below depicts what information is collected from the PIV Applicant in relation to each of these PIV processes. There is no shared enrollment using resources or processes with any other agency.

[1] PSAMS, as it is otherwise known, is the Department's background check database. A PIA is in progress as of this PIA's publication.

Figure 1: Information collected from the PIV Applicant for card issuance

	Identity Proofing and Registration	**IDMS** (Electronically Stored)	PIV Card (Physically Displayed)	PIV Card (Electronically Stored)
Date of birth	X	X		
Place of birth				
Social Security Number (SSN)	X	X		
Other names used				
Citizenship				
Mother's maiden name				
Other identifying information (height, weight, hair color, eye color, gender/sex)				
Organizational affiliation (e.g., Agency name)	X	X	X	X
Employee affiliation (e.g., Contractor, Active Duty, Civilian)	X	X	X	X
Fingerprints (10)	X	X		
Biometric identifiers (2 fingerprints)	X	X		X
Digital color photograph	X	X	X	X
Digital signature [2]		X	X	X
Telephone numbers		X		
Spouse (current or former), relatives and associates, information regarding their citizenship				
Marital status				
Employment history				
Address history		X[3]		
Educational history				
Personal references				
Military history/record				
Illegal drug history				
Criminal history				
Foreign countries visited				
Background investigations history				
Financial history				
Association history				
Signed PIV Request		X		
Signed SF 85 or equivalent		X		
Copies of identity source documents		X		

[2] Public key infrastructure (PKI) digital certificate with an asymmetric key pair.

[3] Please note only the Applicant's current address, extracted from the PIV Request Form, is retained in IDMS.

1.2 What is the information used for?

The information identified above as being collected is used in each step of the PIV issuance process as described below:

1. **Conduct a background investigation.** The PIV background investigation as required by FIPS 201 is a condition of Federal employment (now extended to contractors) and matches PIV Applicants information against FBI and IAFIS databases to prevent the hiring of applicants with a criminal record or possible ties to terrorism. If persons decline providing this information, they cannot be hired as a permanent employee, nor work at the agency as a contractor long-term (over 6 months). Two paper-based forms are used to initiate the background investigation, Questionnaire for Non-Sensitive Positions Standard Form 85 (SF-85) or the Questionnaire for National Security Positions Standard Form 86 (SF-86).[4] This process entails conducting a full National Agency Check (NAC) or National Agency Check with Inquires (NACI), which are described below:

   - **NAC:** Consists of searches of the OPM Security/Suitability Investigations Index (SII), the Defense Clearance and Investigations Index (DCII), the Federal Bureau of Investigation (FBI) Identification Division's name and fingerprint files, and other files or indices when necessary.
   - **NACI:** The basic and minimum investigation required on all new Federal employees consisting of a NAC with written inquires and searches of records covering specific areas of an individual's background during the past five years.

It is important to note that the background information collected as part of this process and its results are kept in the background investigation files; however, it is not stored on the PIV card.

2. **Complete the identity proofing and registration process.** The biographic information collected as part of this process is used to establish the PIV applicant's identity. Biometrics are used to ensure PIV Applicants have not been previously enrolled in the DHS PIV system. As part of this process, FIPS 201 requires that Applicants provide two forms of identity source documents in original form. The identity source documents must come from the list of acceptable documents included in Form I-9, OMB No. 115-0316, Employment Eligibility Verification.[5] PIV Applicants will also participate in an electronic signature process conforming to the Electronic Signature (ESIGN) Act. This confirms presentation of and agreement with the privacy notice, confirms the intent to participate in the PIV process, and submit to a named-based threat background check as required depending on job requirements.

3. **Create a data record in the PIV Identity Management System (IDMS).** The IDMS is used during the registration process to create the PIV Applicant's pre-enrollment and enrollment record, manage and maintain this information throughout the PIV card lifecycle, and, verify, authenticate and revoke PIV cardholder access to federal resources. A unique identifier is assigned during registration and used to represent the individual's identity and associated attributes stored in the system.

4. **Issue a PIV card.** A PIV card is issued upon successful completion of the background investigation and the identity proofing and registration process, and successful completion of the enrollment process. Biometrics are used during PIV card issuance to verify PIV Applicant identity and complete activation of the card. This provides much stronger security assurances than typical card activation protections such as Personal Identification Numbers (PINs) or passwords. Once the

[4] SF 85 and SF 86 can be downloaded at: http://www.opm.gov/forms/html/sf.asp
[5] Form I-9 can be downloaded at: http://uscis.gov/graphics/formsfee/forms/i-9.htm

individual has been issued a PIV Card, the IDMS is updated to reflect that the card has been issued. The issued PIV card cannot be used for access to DHS facilities and networks until activated at the participating location, by the local facility operator.

5. **Usage of PIV Card for physical and logical access:** The biometrics collected are used to verify that the rightful cardholder is presenting the card in relation to physical and logical access to federal facilities and information (i.e., computers). The biographic and other information displayed on the PIV card is used by physical security guards for identity verification purposes.

1.4 How is the information collected?

Information is collected in paper and electronic form.

1.5 What other information is stored, collected, or used?

Additionally, the DHS PIV IDMS and PIV cards contain other data not collected from the PIV Applicant that are (i) electronically stored on the card, (ii) electronically stored in the IDMS, and/or (iii) physically displayed on the card. This information and the purpose of its use is described in Figure 2 below.

Figure 2: Other PIV Information stored, collected or used

	IDMS (Electronically Stored)	PIV Card (Physically Displayed)	PIV Card (Electronically Stored)	Purpose
Card expiration date	X	X	X	To verify card is valid and allow access to facilities and computer systems
Personal Identification Number (PIN)			X	To be used for physical access to highly secured buildings/ space or to log-on to sensitive computer systems ("level 3") that require multi-factor authentication, beyond the typical user ID/ password.
Agency card serial number	X	X		For tracking and maintaining agency cards
Issuer identification number		X		Verify issuers authority
Contact Integrated Circuit Chip (ICC)			X	Used to authenticate a PIV cardholder's identity with card readers that require card to be inserted or "swiped To be used for physical access to buildings/office space and logical access to computer systems.
Contactless ICC			X	Used to authenticate a PIV cardholder's identity with low-frequency radio signal "proximity loop" card readers that allow card to pass by the card reader. Use is for physical access to buildings/office space.

	IDMS (Electronically Stored)	PIV Card (Physically Displayed)	PIV Card (Electronically Stored)	Purpose
PIV authentication key			X	Used to authenticate the PIV card to the host computer system in relation to validating a PIV cardholder's identity.
Cardholder Unique Identifier [Federal Agency Smart Card Credential Number (FASC-N)]			X	Used to authenticate the cardholder to the host computer system and is comprised of the agency code plus a sequential number for the employee, creating a unique number for all Federal employees. This allows interoperability of the PIV card throughout the Federal Government.
PIV Registrar Approval (digital signature)	X			Used to verify the authenticity of the individual sending the message, and verifies the content has not been altered.

1.6 Does the PIV program utilize or depend on the use of commercial databases or commercially available data?

No.

1.7 Will new or previously unavailable information about an individual be obtained or generated? If so, what will be done with the newly derived information? Will it be placed in the individual's existing record? Will it be placed in an existing system of records? Will a new system of records be created? Will the agency use the newly obtained information to make determinations about the individual? If so, explain fully under what circumstances that information is used and by whom.

New information is created when the determination as to whether to issue the PIV is made. Information created from clearance procedures will be used in regard to card issuance or revocation.

1.8 What privacy risks did the agency identify regarding the amount and type of information to be collected and describe how the agency mitigates those risks.

The Department was required to follow specific guidelines regarding the scope of information collected. This is because certain information is required for a background check based on Office of Personnel Management standards and FIPS 201 in support of the NIST 800-79, Guidelines for the Certification and Accreditation of PIV Card Issuing Organization. The Department has sought to collect no

more information than is necessary for a properly conducted background check and the issuance of the card. As indicated in Figure 1, DHS collected only the information required for its needs.

Section Two: Internal Sharing and Disclosure

2.1 What information is shared with which internal organizations and what is the purpose?

The information is shared with the appropriate Department employees and contractors involved in the design, development, implementation and execution of the Department's PIV program who, by law and contract, are bound by the Privacy Act and Departmental policies regarding the handling and removal of personally identifiable information. Specific information about a PIV Applicant or Cardholder will be shared with Department employees and its contractors who have a "need to know" for implementation of the Department's PIV Program. Department contractors are contractually obligated to comply with the Privacy Act in the handling, use, and dissemination of all personal information.

OCIO is actively working to use the connectivity between US-VISIT's IDENT system and Department of Justice/FBI's system to send the fingerprints directly to the Department of Justice/FBI. Department of Justice/FBI would then provide the results as indicated back to DHS. It is anticipated that this connectivity will be in place by December 2006.

Currently the PIV program is in a phased rollout and will only encompass personnel DHS Headquarters. The program will eventually encompass personnel at all components. This PIA will be updated as new components come online.

2.2 For each internal organization, what information is shared and for what purpose?

When components come online they will collect all of the information detailed in question 1.1.

2.3 What roles are associated with the operation?

The critical roles associated with the Department's PIV identity proofing, registration and issuance processes are described below. All individuals are trained to perform his or her respective role; however, these roles may be ancillary roles assigned to personnel who have other primary duties.

1. **PIV Sponsor:** This is the individual who substantiates the need for a PIV credential to be issued to the Applicant and provides sponsorship to the Applicant. The PIV Sponsor requests the issuance of a PIV credential to the Applicant. PIV Sponsors shall meet the following minimum standards: (i) be a Federal Government employee and be authorized in writing by the Bureau, Organization or Regional Office to request a PIV credential; (ii) has valid justification for requesting a PIV credential for an Applicant; (iii) be in a position of responsibility for the Bureau, Organization or Regional Office; and (iv) has already been issued a valid PIV credential.

The PIV Sponsor completes a PIV Request for an applicant and submits to the PIV Registrar and the PIV Issuer. The PIV Request includes the following information:

- Name, organization, and contact information of the PIV Sponsor, including the address of the sponsoring organization;

- Name, date of birth, position, and contact information of the Applicant and contact information of the designated PIV Registrar;
- Name and contact information of the designated PIV Issuer;
- Signature of the PIV Sponsor.

2. **PIV Registrar:** This is the entity responsible for identity proofing of the Applicant and ensuring the successful completion of the background checks. The PIV Registrar provides the final approval for the issuance of a PIV credential to the Applicant. PIV Registrars shall meet the following minimum standards: (i) is a Federal Government official and is designated in writing as a PIV Registrar; (ii) is capable of assessing the integrity of the Applicant's identity source documents (i.e., is trained to detect any improprieties in the applicant's identity-proofing documents) and (iii) is capable of evaluating whether a PIV application is satisfactory and apply organization-specific processes to an unsatisfactory PIV application. Thus, the PIV Registrar needs training on organization processes and procedures for evaluating an unsatisfactory PIV application.

The PIV Registrar has access to the following information:

- Applicant's SF 85, or equivalent; and
- Two forms of identity source documents

The PIV Registrar will record the following data for each of the two identity source documents, sign the records and keep it on file:

- document title (e.g. U.S. Passport; Birth Certificate);
- document issuing authority;
- document number;
- document expiration date (if any); and
- any other information used to confirm the identity of the applicant.

The PIV Registrar:

- Compares the applicant's PIV request information (name, date of birth, contact information) with the corresponding information provided by the applicant at an earlier visit.
- Captures a facial image of application and retains a file copy of the image.
- Fingerprints the applicant and retains a copy.
- Initiates a NACI.
- Notifies the PIV Sponsor and designated PIV Issuer that applicant had been approved or not.

3. **PIV Issuer:** This is the entity that performs credential personalization operations and issues the identity credential to the Applicant after all background checks, identity proofing, and related approvals have been completed. The PIV Issuer is also responsible for maintaining records and controls for PIV credential stock to ensure that stock is only used to issue valid credentials.

The PIV Registrar makes available following information to the PIV Issuer:

- Facial image,
- Copy of result of background investigation, and
- Approval (or disapproval) of the determination and adjudication results.

4. **PIV Digital Signatory:** This is the entity that digitally signs the PIV biometrics and the Card Holder Unique Identifier (CHUID). This role applies for PIV-II, the standards in support of the technical interoperability requirements described in HSPD-12. The PIV Registrar makes available to the PIV Digital Signatory:

- Electronic biometric data for card personalization

5. **PIV Authentication Certification Authority (CA):** The Certification Authority that signs and issues the PIV Authentication Certificate. This role applies to the standards in support of technical interoperability requirements for PIV-II.

6. **PIV Adjudicator:** The entity responsible for determining whether the Applicant is suitable to receive a credential, based on results obtained from the OPM background investigation. Adjudicator responsibilities include: (i) confirming fingerprint results from OPM/FBI; (ii) adjudicating NACI (or higher level OPM investigation) and resolving issues if necessary; (iii) providing final results to the PIV Registrar; and (iv) updating the Official Personnel File (OPF) or Contract file with "Certificate of Investigation."

7. **Enrollment Official (EO):** The individual responsible for performing identify-proofing for applicants at locations that do not have a PIV Card Issuing Facility (PCIF), or direct access to the Human Capital Office (for Federal) or a Hiring Manager (for contractor/Associates). The EO verifies the claimed identity of the applicant, creates the registration package to be submitted to the DHS for registration and enrollment and issues the personalized PIV credential to the applicant.

8. **PCIF Manager:** The PCIF Manager is responsible for each PCIF Facility and ensures that all the services specified in FIPS 201 are provided reliably and that PIV credentials are produced and issued in accordance with its requirements.

9. **System Administrator:** The OCIO or its designee is responsible for the administration of the system, servers and workstations.

2.4 How is the information transmitted or disclosed?

All data is shared electronically and is encrypted to be in compliance with departmental policies in connection with OMB Memorandum M-06-16.

2.5 Given the internal sharing, discuss what privacy risks were identified and how they were mitigated.

Currently the PIV program is not in a phase where components are using the system; however, based on OMB and NIST standards, as well as DHS's own review, detailed security measures are already being prepared to ensure effective but secure information sharing. Once PIV internal information sharing is prepared to be rolled out this PIA will be updated to detail the security measures. Section 7, specifically question 7.2, details the measures already in place.

Section Three: External Sharing and Disclosure

3.1 What information is shared with which external organizations and what is the purpose?

During the up-front background investigation process and identity proofing, relevant personal data will be:

1. Shared with the OPM who is responsible for conducting the NACI and other higher-level investigations for DHS; and
2. OPM shares with Federal Bureau of Investigation (FBI) who matches against databases to prevent the hiring of applicants with a criminal record or national security concerns, including possible ties to terrorism.

Additionally, information about individuals that is stored for purposes of issuing a PIV card and to run the DHS PIV program may be given without individual's consent as permitted by the Privacy Act of 1974 (5 U.S.C. § 552a(b)), including to:

- an appropriate government law enforcement entity, if records show a violation or potential violation of law;
- the Department of Justice, a court, or other adjudicative body when the records are relevant and necessary to a law suit;
- a federal, state, local, tribal, or foreign agency whose records could facilitate a decision whether to retain an employee, continue a security clearance, or agree to a contract;
- a Member of Congress or to Congressional staff at a constituent's written request; to the Office of Management and Budget to evaluate private relief legislation;
- agency contractors, grantees, or volunteers, who need access to the records to do agency work and who have agreed to comply with the Privacy Act;
- the National Archives and Records Administration for records management inspections; and
- other federal agencies to notify them when a PIV card is no longer valid.

The full System of Records Notice (SORN) with complete description of routine uses was published in the Federal Register at cite and can be viewed at: System of Records Notice, 71 Fed. Reg. 53697 (Sept. 12, 2006); Notice of Proposed Rulemaking, 71 Fed. Reg. 53609 (Sept. 12, 2006).

3.2 How is the information transmitted or disclosed?

Information is transmitted electronically.

3.3 Is a Memorandum of Understanding (MOU), contract, or any agreement in place with any external organizations with whom information is shared, and does the agreement reflect the scope of the information currently shared?

OPM is designated as the principal provider of background investigations to all federal agencies unless an agency has been given delegated or legislative authority to conduct its own background investigations. As part of the background investigation, each subject is required to submit forms containing their personal information. Providing this data is voluntary but the submitting the information is required to proceed with the necessary background investigation that underpins their federal service.

The SF86 (for National Security positions) and the SF85P (for Public Trust positions) are the specific forms used to capture the information regarding the particular subject. Each of these forms has a section in the instructions that discuss the purpose of the investigation and the government's requirement to protect the data from unauthorized disclosure. Additionally, the form describes how the collected information and information from the background investigation may be disclosed without specific consent as permitted by the Privacy Act and the routine uses of such data.

These statements, and the underlying authorities (e.g. Executive Orders (10450 and 12968) and law (5 CFR 731, 732, and 736)) are what govern the collection, transmission, and reporting of data. There are Interagency Agreements with OPM for both the background investigations and fingerprinting (currently processed through OPM) that outline the information sharing.

3.4 Is the Department either providing or receiving card issuance services pursuant to a serving agreement?

No.

3.5 How is the shared information secured by the recipient?

As the designated organization for background checks, OPM must follow FISMA and has appropriate security measures in place to ensure proper access to information and the security of personnel records.

3.6 What type of training is required for users from agencies outside DHS prior to receiving access to the information?

OPM employees are required to receive privacy and security training.

3.7 Given the external sharing, what privacy risks were identified and describe how they were mitigated.

DHS has agreements in place with OPM to ensure that there are formal procedures in place to secure and protect DHS employee and contractor data. OPM is required not only by the Agreements with DHS but also by government-wide security standards to ensure that any information it receives or transmits is transmitted to a party who has a need to know and that the receiving party has adequate security measures in place. Although there are always risks of unauthorized disclosure when transmitting data

electronically, DHS and OPM have taken all necessary and reasonable measure to ensure that such events do not take place.

Section Four: Agency Policy Requirements

The Department has followed DHS Management Directive (MD) 11042.1 Safeguarding Sensitive and Unclassified Information (FOUO), and DHS Policy for FOIA Compliance MD 0460.1. As additional policies related to the HSPD-12 program, e.g., Biometric Privacy (see NSTC Subcommittee on Biometrics Report, April 2006), are developed, it is expected that DHS Management Directives will be issued.

Section Five: Privacy Act Requirements

5.1 Is notice provided to the individual at the time information is collected? If yes, provide or attach the Privacy Act Statement. If notice is not provided, why not?

In all cases, PIV applicants are provided a notice required by the Privacy Act, 5 USC § 552(a)(e)(3). The notice states the reasons for collecting information, the consequences of failing to provide the requested information, and explains how the information is used. The collection, maintenance, and disclosure of information comply with the Privacy Act and the published System of Records Notices (SORN) for the PIV program, DHS-OS-001, Office of Security File System, and DHS-OS-2006-047, Personal Identity Verification Management System (PIVMS). (System of Records Notice, 71 Fed. Reg. 53697 (Sept. 12, 2006); Notice of Proposed Rulemaking, 71 Fed. Reg. 53609 (Sept. 12, 2006)).

PIV applicants using an electronic signature process conforming to the Electronic Signature (ESIGN) Act, confirm presentation of and agreement with the Privacy Act Statement and agree to participate in the PIV process and submit to a named-based threat background check appropriate to job requirements.

5.2 What are the procedures for individuals to gain access to their own information?

Release of information to individuals would be in compliance with the Privacy Act, 5 U.S.C § 552a; DHS Privacy Act Regulations, 68 FR 4056; and the DHS FOIA process established in accordance with EO 13392. FOIA and Privacy Act requests should be mailed to Department Homeland Security, Catherine Papoi, Acting Director, Departmental Disclosure Office and & FOIA, Privacy Office, Department of Homeland Security, Washington DC 20528.

Individuals may directly correct basic information such as address and phone number at any time after the clearance process is completed. This will be completed through a DHS website with manager approval of each change; however, during the clearance process individuals may not directly alter their information. They may inform the DHS Security Office of a change in their information, but may not directly access their information.

5.3 What are the procedures for correcting information?

The DHS HSPD-12 Procedures Reference Book establishes the process by which an individual may correct his/her own information. The information provided by the applicant during the pre-enrollment and enrollment processes has been verified and authenticated, and changes to the database would occur for a name change or for additional information provided through adjudication procedures. The cardholder completes and submits the necessary change documentation to Human Capital and after acquiring the appropriate authorized signatory takes a completed 11000-14 form to the ACO, to whom the cardholder presents their existing DHS PIV card, proof of name change documentation provided to PSD or Human Capital. The ACO reviews DHS Form 11000-14 for completeness and approval, searches the IDMS to locate the cardholders record, verifies that the DHS PIV is currently valid. The ACO instructs the cardholder on steps for determining biometric match, performs matching (usually on fingerprints), authenticates the cardholders identity using the standards of FIPS 201. The PIV issuer revokes the existing card; verifies the cardholder's IDMS record digital photograph; scans the name change into the cardholders file in the IDMS; recaptures the biometrics; provides the cardholder with the DHS PIV Cardholders Responsibilities documentation; prints the new DHS PIV card; ensures its correct functioning; and issues the card to the cardholder. The cardholder acknowledges, through digital signature, that he/she has received the DHS PIV card and documentation on related responsibilities.

Accuracy of an applicant's data is checked in the Pre-enrollment process by the Personal Security Division (PSD) security assistant during review of the sponsor (Human Capital) provided DHS Form 11000-5 , and in the Enrollment process by the Enrollment Official (EO).

The DHS HSPD-12 Procedures Reference Book provides for additional procedures to reduce inaccuracies in submitted documents through the requirement that the PSD security assistant search the PSAMS to verify information, and in the enrollment process, both through visual and electronic validation of the authenticity of source documents.

5.4 How are individuals notified of the procedures for correcting their information?

Individuals are informed in writing at the time of enrollment of the procedures for correcting data. Additionally, before receiving a card, the form used for issuance of the actual card contains notice reminding the employee or contractor of the ability access information as well as notice of the uses of the collection.

5.5 If no opportunity to amend is provided, what alternatives are available to the individual?

Opportunities to amend are provided (see 5.2 and 5.3).

5.6 Do individuals have the right to decline to provide information?

By signing the PIV application form, applicants acknowledge that the DHS may use their information as outlined in the Privacy Act Statement and associated Privacy Act SORN. While there is no legal requirement to use a PIV Card, employees who do not use a PIV Card will be treated as visitors when

entering a federal building and will be barred from access to certain federal resources. If using a PIV card is a condition of the job, withholding requested information will affect job placement and/or employment prospects.

5.7 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

Individuals are notified of the uses of their information prior to collection. Once the information is given, the individual has given consent to the uses. The DHS Security Office will not use the information outside of the uses outlined in this PIA, the System of Records Notice, and the notice provided on the relevant forms. Should DHS anticipate a need for a new use for the information the PIA, SORN and form notices will be updated.

5.8 What deficiencies in your agency procedures did you remedy after performing this analysis?

The critical analysis of notice procedures determined that there is a sufficiency of notice for use and information correction procedures through the certification of the process and system before operability in accordance with the Privacy Act. Additionally, it was noted that should uses of the information change there are legal notice requirements that must mirror the collection and use practices. No use and collection changes will occur without updates to the appropriate documentation.

Section Six: Data Protection Controls

DHS has implemented general program controls to ensure the privacy and security of the data. This includes:

- The Applicant appears in-person at least once before the issuance of a PIV credential.
- The PIV identity proofing, registration and issuance process adheres to the principle of separation of duties to ensure that no single individual has the capability to issue a PIV credential without the cooperation of another authorized person.
- The identity proofing and registration process is accredited by DHS Chief Security Officer as satisfying the requirements and approved in writing by the head of the Federal department or agency.
- DHS issues PIV credentials only through the IDMS systems which has an Authority To Operate of 10/13/2006.
- DHS conducted this PIA consistent with the E-Government Act and the Homeland Security Act of 2002.
- DHS has generated a SORN identifying the type of information collected, the purpose of the collection how the information is protected, and the complete set of uses of the credential and related information during the life of the credential.

- DHS Office of Security coordinates with the DHS Privacy Office to define consequences for violating privacy policies of the PIV program.
- DHS utilizes technologies that allow for continuous auditing of compliance with stated privacy policies and practices governing the collection, use and distribution of information in the operation of the program.
- DHS utilizes security controls described in NIST SP800-53, Recommended Security Controls for Federal Information Systems, to accomplish privacy goals, where applicable.

6.1 What are the controls on data exchange and integrity of the credential?

NIST has documented security for HSPD-12 systems in FIPS 201. The DHS implementation is in compliance with Departmental and regulatory requirements including both the system and PIV credential security. Audits will be performed under the direction of the PCI manager to ensure the integrity of the PIV system. Both electronic and physical access to the system is controlled.

System security: The risks include the electronic security of the transmission networks and the physical and visual security of the systems and locations in the agency facility where the information is stored. These risks are addressed by the IT Security Plan established for the PIV program. More specific program controls include protecting data through the use of FIPS compliant encryption algorithms in transit and at rest.

Networks: The IT infrastructure that supports the PIV program is described in detail in the IT Security Plan. All data exchange takes place over encrypted data communication networks that are designed and managed specifically to meet the needs of the PIV Program. Private networks and/or encryption technologies are used during the electronic transfer of information to ensure that Internet "eavesdropping" cannot occur and that data is sent only to its intended destination and to an authorized user by an authorized user. Enrollment data may be temporarily stored at enrollment centers for encrypted batch transmission to the IDMS.

Databases: The OCIO identifies the administrative, operational and technical controls (Privacy Act and E-Government Act) applied to protect this IDMS data repository containing biographical data, photo images and biometric identifiers. These controls are designed into the IDMS and the PIV infrastructure to mitigate privacy risk. The specific-access restrictions based are role-based and authentication is required.

Data Transmission: Biometric image data collected at enrollment centers are handled as sensitive personal information throughout the process. Biometric images are stored as compressed and encrypted data and are completely disassociated from personally identifiable information. The IDMS generates an "index key" that serves as the only link between an enrolled individual's biographical information and biometric image data. In addition, biometric images and the biometric templates created from this data are suitably controlled to prevent any interception, alteration, release, or other data compromise that could result in unauthorized use. Biometric protection techniques outlined in International Committee for Information Technology Standards (INCITS) Standard - 383 are used to secure these biometric templates. Under no circumstances is any biometric data retained in the local enrollment station after transmission to the IDMS is complete. Enrollment centers do not retain any information. System design and architecture supports the automatic deletion of all collected information (e.g., enrollment record) after successful

transmission to the IDMS. The confirmation of deletion produces an auditable record of the event for verification.

Data Storage Facilities: Facilities and equipment are secured by limiting physical access to the workspace and system, and by requiring an appropriate verification of identity for logical access to the system. Where appropriate, this method uses the PIV card providing one, two or three factors of authentication (i.e., something you have, something you know and something you are). Where necessary, this method also consists of two components (e.g., user id + password).

The IDMS sends confirmed enrollment information to the card production facility via a private connection. Cards that are not active cannot be used for access to federal facilities or networks. Certifications are revoked when they are reported lost, stolen, damaged beyond use, or when a cardholder has failed to meet the terms and conditions of enrollment. Cards will be deactivated upon collection of damaged cards or if the employee or contractor no longer requires a PIV card.

Equipment: PIV cardholders are authenticated to access the PIV system using, at a minimum, two-factor authentication based on their role and responsibility. A required component (first factor) of this authentication is the PIV card itself. In combination with the PIV, the second factor of this authentication requires a personal ID number, pin and/or biometric (e.g., fingerprint.)

User Groups: System/application users have varying levels of responsibility and are only allowed to access information and features of the system appropriate for their level of job responsibility and security clearance. These rights are determined by the identification provided when authenticating (i.e., user identification) to the system as described above.

Network Firewall: Equipment and software are deployed to prevent intrusion into sensitive networks and computers.

Encryption: Sensitive data are protected by rendering it unreadable to anyone other than those with the correct keys to reverse the encrypted data.

Audit Trails: Attempts to access sensitive data are recorded for forensic purposes if an unauthorized individual attempts to access the information contained within the system.

Recoverability: The system is designed to continue to function in the event that a disaster or disruption of service should occur.

Physical Security: Measures are employed to protect enrollment equipment, facilities, material, and information systems that are part of the PIV program. These measures include: locks, ID badges, fire protection, redundant power and climate control to protect IT equipment that are part of the PIV program.

A periodic assessment of technical, administrative, and managerial controls to enhance data integrity and accountability.

System users/operators are officially designated as agents of the DHS and complete a training process associated with their specific role in the PIV process.

Separation of Duties Controls: The PIV Applicant, Sponsor, Registrar, PIV issuer and PIV Digital Signatory roles are exclusively drawn and the agency ensures that these roles do not overlap through the restricted role-based access and authentication requirements.

Security of ID credential issued to an employee or contractor is achieved by full compliance with the mandatory requirements of the Federal Information Processing Standard Publication 201(FIPS Pub 201), Personal Identity Verification of Federal Employees and Contractors. Specific safeguards include:

Card issuing authority limited to providers with official accreditation pursuant to NIST Special Publication 800-79, Guidelines for the Certification and Accreditation of PIV Card Issuing Organizations

Cards use at least one visual tamper proof feature such as holograms, watermarks, etc.

Card data is encrypted and stored on the card.

Card is sheathed in electromagnetically opaque sleeve to protect against unauthorized contact-less access to stored information.

Employees are alerted to importance of protecting card.

Card expiration within 3 years from issuance.

Return of cards to agency when no longer needed (or upon employee/contractor separation from the agency).

Deactivation of card within 18 hours (the latest) of employee/contractor separation, loss of card, or expiration.

Removal of all personally identifiable information associated with the cardholder from the system upon deactivation if cardholder will not be reissued a new card).

Specialized role-based training for all persons involved in the PIV process.

6.3 Who will have access to the information?

Authorized information technology (IT) personnel or contractors (pursuant to an appropriate routine use) who handle the operations and maintenance of the system will have limited access to the system to support the credentialing activity as well as trouble shoot technical system issues encountered on a day-to-day basis. Additionally, the DHS Office of Inspector General (OIG) may request and be given access to the data, and the DHS Office of the General Counsel's may request and be given access to the data to represent DHS in litigation matters related to the PIV system. The described access by OIG and OGC is authorized by section (b)(1) of the Privacy Act.

6.4 Are written procedures in place identifying who may access the system ?

All DHS employees and assigned contractor staff will receive appropriate privacy and security training and have any necessary background investigations and/or security clearances for access to sensitive, privacy or classified information and secured facilities. The DHS ensures this through legal agreements with its contractors and enforcement of internal procedures with all DHS entities involved in processing the background checks. Additionally, robust standard operation procedures and system user manuals describe in detail user roles, responsibilities and access privileges.

6.5 What technical and/or operational controls are in place to prevent misuse of data by those having access?

By design, and for security and privacy reasons, no enrollment data is stored at or by the enrollment workstation or center. The enrollment record can only be viewed or retrieved by a DHS Enrollment Official or PIV Issuer who is trained and authorized to perform enrollment activities. The ability to retrieve or view an employee's enrollment record is controlled by user authentication, which ensures only those with a need to access the data and who possess proper training can retrieve or view enrollment information. In addition to this access control, physical privacy protections will be used. These physical protections include the use of "Privacy Screens" that prevent passers-by from viewing enrollment record information that may be displayed on the enrollment center workstation. Additionally, the enrollment center's physical security controls will be enforced to ensure that only DHS employment officer or PIV issuer with a need for access can enter the enrollment center and view personal information displayed on screens.

6.6 Given the access and security controls you evaluated, what privacy risks were identified and describe how you mitigated them.

The system is established in accordance with and is compliant with the NIST 800-79[6] and FIPS-201[7]. Mitigation of risk is provided by the establishment of the specific roles that determine who receives access to the system and the specific scope of that access.

Section Seven: Data Storage And Retention

7.1 What are the retention periods for the data in the system?

The information collected to issue a PIV card is retained and used after an individual's separation in accordance with National Archives and Records Administration (NARA) General Records Schedule for records pertaining to this program relevant to both the PIV-I and PIV-II.

Records relating to persons' access covered by this system are retained in accordance with General Records Schedule 18, Item 17 approved by the National Archives and Records Administration (NARA). Unless retained for specific, ongoing security investigations, for maximum security facilities, records of

---

[6] Guidelines for Certification and Accreditation of PIV Issuing Organizations

[7] *Personal Identity Verification of Federal Employees and Contractors*, was developed to satisfy the requirements of HSPD 12, approved by the Secretary of Commerce, and issued on February 25, 2005. FIPS 201 incorporates three technical publications specifying several aspects of the required administrative procedures and technical specifications that may change as the standard is implemented and used. NIST Special Publication 800-73, "Interfaces for Personal Identity Verification" specifies the interface and data elements of the PIV card; NIST Special Publication 800-76, Biometric Data Specification for Personal Identity Verification" specifies the technical acquisition and formatting requirements for biometric data of the PIV system; and NIST Special Publication 800-78, "Cryptographic Algorithms and Key Sizes for Personal Identity Verification" specifies the acceptable cryptographic algorithms and key sizes to be implemented and used for the PIV system.

access are maintained for five years and then destroyed. For other facilities, records are maintained for two years and then destroyed.

All other records relating to individuals are retained and disposed of in accordance with General Records Schedule 18, item 22a, approved by NARA. Records are destroyed upon notification of death or not later than five years after separation or transfer of employee, whichever is applicable.

In accordance with HSPD-12, PIV Cards are deactivated within 18 hours of cardholder separation, loss of card, or expiration. The information on PIV Cards is maintained in accordance with General Records Schedule 11, Item 4. PIV Cards are destroyed by cross-cut shredding no later than 90 days after deactivation.

Section Eight: Results of FISMA Review

8.1 Has the system completed a C&A as required by FISMA or other applicable standards?

The FISMA Certification & Accreditation (C & A) will be completed on October 18, 2006.

8.2 If not, at what stage in the C&A process is the system and what is the anticipated date of the C & A?

The system is in the final stages of completing the C & A process to acquire its Authority to Operate (ATO).

8.3 Has the agency conducted a risk assessment, and identified and implemented appropriate technical, administrative, and operational security controls?

Yes. Controls are identified in the system security plan. Per the C & A process, the Security Office conducted reviews of requirements with the OCIO and Physical Security. The DHS HSPD-12 Program Office worked with Physical Security and Personnel Security to define, draft, and provide the Office of Security Service Level Agreements to the OCIO team. The establishment of supporting databases and physical requirements of the system were addressed. The DHS HSPD-12 Procedures Reference Book was developed to document the details of the system to include the controls that are integral to both the pre-enrollment and enrollment stages of the PIV Card issuance process.

Section Nine: Analysis and Assessment

9.1 Whether or not competing technologies were evaluated, describe how data integrity, privacy, and security were analyzed as part of the decisions made for your system.

The DHS Office of Security continues to work closely with the DHS's OCIO to develop requirements, policies and technical solutions to successfully implement FIPS 201-1 and NIST SP800-79. The HSPD-12 Program Office has on-going procedural and policy discussions with the OCIO, PSD, and Human Capital in which the assurance of data integrity is analyzed and affirmed.

In many instances the Department was required to adopt certain technologies as approved by the Office of Management and Budget (OMB). However, the Department participated in regular meetings and adjunct working groups with OCIO, Office of the Chief Procurement Officer, and Physical Security, as well as meetings with HSPD-12 program representatives from other components within the DHS, which involved the Department in the decision making processes regarding the technologies utilized in its implementation of HSPD-12. The technologies are defined and mandated to specific standards set forth in OMB FIPS 201 and NIST 800-79. The issues of data integrity, privacy and security are continually examined at the DHS to ensure that implementation of the HSPD-12 maintains necessary and adequate controls.

9.2 Did you evaluate competing technologies to assess and compare their ability to effectively achieve system goals?

The technology assessment conducted by DHS followed the guidance of the OMB template for industry development of compliant system technology. General Services Administration procurement and Federal Acquisitions Requirement provisions define procuring parameters for this technology. There are competing companies developing the system components, but they are all under the same standards and guidelines for the system to be interoperable government-wide.

9.3 If applicable, describe the competing technologies.

The Department is satisfied with the technological solutions adopted by the many working groups, committees, and ultimately OMB regarding the HSPD-12 implementation. DHS is in the position of being a new and large agency that has merged many different practices and customs into a single unified entity. The technologies adopted and utilized in the PIV effort incorporate DHS's many security needs and requirements.

As the PIV program moves into the components' hands, privacy and security concerns will be examined regularly to ensure that the technology implemented is done so with compliance to DHS's security needs as well as respecting employee and contractor personal privacy.

9.4 Changes made to the PIV process due to this assessment.

No significant changes were made to the PIV process as DHS has implemented it because of this assessment; however, the PIV Program Office has had regular dialogue with the DHS Privacy Office regarding the implementation of DHS's PIV program. Because much of the technology was pre-selected by OMB, DHS had limited opportunity change the PIV process; however, DHS was involved in the discussion groups and meetings centering on PIV product selection and implementation strategies (see 9.1-9.3).

9.5 What unique issues does this system present?

As discussed more fully in question 9.7, there are two major issues presented in the implementation of HSPD-12. First is ensuring the personal information collected for the background check is secure (see Section 1 and Section 6). The second issue PIV presents is the use of biometrics (in this case fingerprints) as identity verifying information.

9.6 What specific strategies are used to address these issues?

Regarding the database of background check information, DHS utilizes separation of access capabilities based on process roles. The Department ensures that only individuals who are authorized to see and have access to the employee information in fact do so. The internal audit process will be defined and implemented commensurate with the completion of the NIST 800-79 C&A at Headquarters in mid-October (10/17/06). The external audit process will be defined and implemented with the component roll-out commencing January 31, 2007, and continuing thereafter.

Audit logs will be established and regularly verified to ensure the possibility of a breach is minimized, if not nullified. Should a breach occur the DHS has a plan in place to immediately respond to the breach. The HSPD-12 Procedures Reference Book addresses the process by which an individual whose card is compromised through being lost, stolen or damaged is to report the event to Security.

A provision for a "match-on" biometric on the card provides for additional security to prevent fraudulent use of cards. Realizing that identity theft and/or unauthorized use of an individual's access card may occur simply through the existence of the card, DHS has a procedure in place if the card is lost, stolen, or damaged. The biometric identifier insures that anyone other than the individual to whom the card is issued will not be able to access any facility in the HSPD-12 program.

9.7 What unique issues are not mitigated completely? What are the potential impacts of these issues on privacy?

Overall HSPD-12 has solved more security and privacy concerns than it has created. There will always be risks associated with the storage of large amount of employee data and transmission, but robust technical controls and sharing protocols are in place to ensure unauthorized access is minimized and data integrity is kept at paramount importance.

Section Ten: Conclusions

The PIV program and all government HSPD-12 efforts have been under intense scrutiny from OMB and Department leadership. DHS has been involved in the selection of products and parameters from the outset of the HSPD-12 efforts. OMB ultimately made determinations on the range of products and solutions DHS could utilize, but DHS had input into the many committees and working groups designed to allow Departments to voice their concerns and needs.

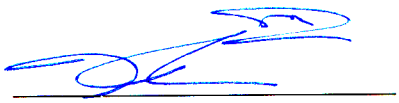
Considerable consideration has been given in establishing the DHS HSPD-12 PIV system to ensure that the system is compliant with applicable E-Government of 2002, Privacy Act of 1974 and Freedom of Information Act provisions, and the PIV Program has worked closely with the DHS Privacy Office and the Chief Information Officer to ensure all requirements have been met in a timely manner.

Responsible Officials

Cynthia Sjoberg
Program Manager, HSPD-12
Training and Operations Security Division
Office of Security
Department of Homeland Security
(202) 447-5010

Homeland Security

Approval Signature Page



Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security

Homeland Security

Appendix A: Privacy Impact Assessment for Personal Identity Verification

PIV Program PIA Reference Sheet

Unique Project Identifier Number (UPI): None
(If no UPI, please explain why.): An OMB300 is not required.

System of Records (SOR) Number: DHS-2006-0047
SORN Title: Personal Identity Verification Management System

Legal Authority(ies): Privacy Act of 1974, E-Government Act of 2002, Homeland Security Presidential Directive 12 (HSPD-12), Federal Information Processing Standard 201: Policy for a Common Identification Standard for Federal Employees and Contractors

IT Security Plan Number(s): Not yet assigned
IT Security Plan Title: Personal Identity Verification System
Accreditation and Certification Date: Pending

OMB Exhibit 300 Number: N/A
OMB Exhibit 300 Title: N/A

Identity Proofing and Registration Process Approval Date: Certification pending

PIV Implementation Plan Approval Date: 09/09/2005

Contact Name, Title: Cynthia Sjoberg, DHS HSPD-12 Program Manager

E-Mail: Cynthia.Sjoberg@dhs.gov

Organization/Department: Training and Operations Security Division, Office of Security, U.S. Department of Homeland Security

Phone Number: (202) 447-5324

Activity/Purpose of Program: To store, manage, and maintain information related to the issuance and maintenance of PIV credentials to federal employees and contractors, and, the process of verification and authentication of access to federal resources by federal employees and contractors.