Justice Management Division

Privacy Impact Assessment

for the

Personal Identity Verification (PIV) Card System

Issued by:

Stuart Frisch, Senior Component Official for Privacy

Reviewed by: Vance E. Hitch, Chief Information Officer, Department of Justice

Approved by: Nancy C. Libin, Chief Privacy and Civil Liberties Officer, Department of Justice

Date originally approved: September 19, 2007
Date revision approved: March 24, 2011

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 policy 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. The National Institute of Standards and Technology (NIST) published a standard for secure and reliable forms of identification, Federal Information Processing Standard Publication 201 (FIPS 201), *Personal Identity Verification (PIV) of Federal Employees and Contractors*. The credential is for physical and logical access.

FIPS 201 has two parts: PIV I and PIV II. The requirements 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 specifies standards for implementing identity credentials on integrated circuit cards (i.e., smart cards) for use in a Federal system. Simply stated, FIPS 201 requires agencies to:

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

DOJ Implementation

In response to HSPD-12 and to meet the requirements summarized above, the General Services Administration (GSA) established the HSPD-12 Managed Service Office (MSO) to provide common, shared infrastructure and services to assist federal agencies in the implementation of HSPD-12. DOJ has signed up to use the GSA MSO's shared infrastructure and services. Approximately 25 other federal agencies are also using the GSA managed service. The scope of the GSA managed services consists of enrollment stations, system infrastructure through a centralized PIV Identity Management System (IDMS), card production facility, and card activation, finalization, and issuance. DOJ will use GSA enrollment and issuance stations hosted in DOJ space and staffed by DOJ personnel, which link to the GSA MSO IDMS, card production facility, and other services. DOJ Justice Management Division, Security and Emergency Planning Staff, and Enterprise Solutions Staff are jointly responsible for the identity management and all aspects of the DOJ 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 revision to the September 2007 PIA adds language to describe a tool being used to assist DOJ components to structure data in the correct format as they import data from existing personnel data sources to GSA's USAccess HSPD-12 card system. Use of this tool is temporary and will be phased out when it is no longer needed.

Section 1.0 The System and the Information Collected and Stored within the System.

The following questions are intended to define the scope of the information in the system, specifically the nature of the information and the sources from which it is obtained.

1.1 What information is to be collected?

The biographic and biometric information collected includes: full name, Social Security number, Applicant ID number, date of birth, current address, digital color photograph, fingerprints (10), biometric template (two fingerprints), organization, employee affiliation, work e-mail address, work telephone number, office address, copies of identity source document, employee status, military status, foreign national status, federal emergency response official status, law enforcement official status, results of background check, Government agency code, and PIV card issuance location. Additionally, the PIV Identity Management System (IDMS) and PIV cards contain other data not collected from the PIV Applicant that are either (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 1.

Figure 1: 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	For optional/ selected use either 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 identifying 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 into the reader. Can be used for physical access to

	IDMS (Electronically Stored)	PIV Card (Physically Displayed)	PIV Card (Electronically Stored)	Purpose
				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. Primary use is for physical access to buildings and office space.
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.

1.2 From whom is the information collected?

The information is collected from PIV Applicants, the individuals to whom a PIV card is issued. The PIV Applicant may be a current or prospective Federal employee, or a contractor. Some information is pre-populated in the IDMS based on DOJ human resources data by the applicant's Sponsor.

Section 2.0 The Purpose of the System and the Information Collected and Stored within the System.

The following questions are intended to delineate clearly the purpose for which information is collected in the system.

2.1 Why is the information being collected?

As required by FIPS 201, DOJ will collect biographic and biometric information from the PIV Applicant in order to: (i) conduct the background investigation or other national security investigation for federal employees and contractors; (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, as mandated by HSPD-12. The PIV card issuance process, including background check requirements, and physical and electronic contents of the PIV card are defined by FIPS 201.

2.2 What specific legal authorities, arrangements, and/or agreements authorize the collection of information?

The information is required to meet the requirements of HSPD-12 and FIPS 201.

2.3 Privacy Impact Analysis: Given the amount and type of information collected, as well as the purpose, discuss what privacy risks were identified and how they were mitigated.

The privacy risks identified were compromise of privacy data at the GSA managed service core system, external to DOJ; compromise of privacy data at the DOJ operated enrollment stations; and compromise of data on an individual PIV card. Risks are from both internal (trusted personnel) and external actors.

The risk of data compromise is mitigated by physical, administrative, and technical security measures. All access to data is restricted on a "need-to-know" basis. All access has role based restrictions. Role based access controls are enforced via the use of PIV cards. Individuals with access privileges have undergone vetting and suitability screening and are trained in their responsibilities to protect privacy data. Data is secured physically by locks on doors and locking storage containers. The hosting facility buildings have security guards and secured doors. All entrances are monitored through electronic surveillance equipment. Picture identification badges are required for access to the facility. All data is encrypted in transit between the GSA MSO and DOJ. Secure (encrypted) virtual private networks (VPN) are used from the enrollment stations at DOJ to the GSA servers. GSA maintains an audit trail and performs random periodic reviews to identify unauthorized access. DOJ receives periodic reports which detail card issuances, revocations, and other information on card statistics. These reports are reviewed by Security and Emergency Planning Staff.

Section 3.0 Uses of the System and the Information.

The following questions are intended to clearly delineate the intended uses of the information in the system.

3.1 Describe all uses of the information.

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

- **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 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 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). Note: The background information collected as part of this process and its results are kept in the background investigation files; however, not stored on the PIV card.

- **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 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.[1] 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 name-based threat background check as required depending on job requirements.
- **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.
- **Issue a PIV card.** A PIV card is issued upon successful completion of the background investigation and 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 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 DOJ facilities and networks until activated at the participating location, by the local facility operator or system owner.
- **Usage of PIV Card for physical and logical access:** The biometrics collected can be 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.

3.2 Does the system analyze data to assist users in identifying previously unknown areas of note, concern, or pattern? (Sometimes referred to as data mining.)

[1] Form I-9 can be downloaded at: http://uscis.gov/graphics/formsfee/forms/i-9.htm

No. Biometrics collected from PIV applicants are used to perform a check to ensure that a PIV card has not been previously issued to the same individual.

3.3 How will the information collected from individuals or derived from the system, including the system itself be checked for accuracy?

PIV card applicant data is checked against existing human resources and personnel security data by the sponsor of the applicant. Data is checked against I-9 identity source documents during enrollment. Applicant data is also verified during the background investigation process. Upon submittal from the enrollment station, data is digitally signed to prevent tampering or modification.

3.4 What is the retention period for the data in the system? Has the applicable retention schedule been approved by the National Archives and Records Administration (NARA)?

Disposition of records will be according to NARA disposition authority N1-269-06-1 (pending).

3.5 Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

Only authorized personnel with a "need-to-know" are allowed access to the information. These individuals are trained in their roles on the system to carry out the process described in FIPS 201. The personnel are trained in their responsibilities to protect privacy information. The system records transactions in audit logs which are reviewed for inappropriate activity. No data is stored on the DOJ enrollment workstations. Once an enrollment package is transmitted to the GSA core system, all applicant information is deleted from the enrollment workstations.

Section 4.0 Internal Sharing and Disclosure of Information within the System.

The following questions are intended to define the scope of sharing both within the Department of Justice and with other recipients.

4.1 With which internal components of the Department is the information shared?

The information is entered at enrollment stations staffed by DOJ personnel, and is only shared internally by those filling the roles in the GSA managed service, listed below. DOJ internally fills 1, 2, 6, and 7. During the up-front background

investigation process and identity proofing, relevant personal data will also be matched against databases at the Federal Bureau of Investigations (FBI) to prevent the hiring of applicants with a criminal record or possible ties to terrorism.

The roles are described below.

1. **PIV Sponsor:** 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) is a Federal Government employee and be authorized in writing by DOJ to request a PIV credential; (ii) have valid justification for requesting a PIV credential for an Applicant; (iii) be in a position of responsibility for DOJ; and (iv) have already been issued a valid PIV credential.

   - Using the GSA managed service, the PIV Sponsor completes a PIV Request for an applicant and submits it to the PIV Registrar and the PIV Issuer
   - For the initial effort of sponsoring large numbers of existing employees and contractors for PIV cards, a file containing sponsorship information on multiple individuals can be uploaded to the GSA managed service by the Security Officer, as described below. The individuals' information in the file must first be reviewed and approved by a DOJ Sponsor and Adjudicator before upload. This process is referred to as "bulk upload." Bulk upload files are sent from DOJ to the GSA managed service system over an encrypted interface. The bulk upload process is temporary and will be phased out over time.

2. **PIV Registrar**: This role may be filled by DOJ or GSA personnel. 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 (iv) 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
   - Two forms of identity source documents

   The PIV Registrar logs into an enrollment station and:

- Compares the applicant's PIV request information (name, date of birth, contact information) with the corresponding information provided by the sponsor.
- Captures a facial image of applicant.
- Fingerprints the applicant, obtaining all fingerprints.
- Initiates a NACI, unless NACI has already been completed.
- Notifies the sponsor and designated PIV Issuer that applicant had been approved or not.

3. **PIV Issuer (**GSA Managed Service)**:** This role is described in Section 5, External Sharing and Disclosure.

4. **PIV Digital Signatory (GSA Managed Service):** This role is described in Section 5, External Sharing and Disclosure

5. **PIV Authentication Certification Authority (CA):** This role is described in Section 5, External Sharing and Disclosure

6. **PIV Adjudicator (DOJ):** 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. **Security Officer (DOJ):** The security officer is a DOJ individual authorized to physically collect revoked cards, and is the daily contact for agency employees to report lost, missing, or stolen PIV cards. The security officer is responsible for revoking or suspending PIV cards, if required. The Security Officer can also perform bulk uploads. All information on DOJ personnel in the IDMS can be viewed by the security officer.

4.2 For each recipient component or office, what information is shared and for what purpose?

As described in the section above, each of the roles logs into the GSA Managed Service system to execute their portion of the FIPS 201 card issuance process. The information involved and the purpose of the role is described in the section above. A "least privilege" role-based access system restricts access to data on a need-to-know basis; access to the data is limited to those with an operational need to access the information.

4.3 How is the information transmitted or disclosed?

The information is transmitted from the enrollment station to the GSA IDMS using an encrypted virtual private network. No information is stored on the enrollment stations. The resulting PIV cards are mailed to DOJ. DOJ Sponsors, Adjudicators, and Security Officers access the GSA system using a web browser and an encrypted web session. Sponsorship data for bulk uploads may be prepared using desktop office automation software, such as spreadsheets, or a custom software tool developed to format sponsorship data and produce a bulk upload file. The bulk upload file is sent to the GSA managed service by a Security Officer over an encrypted connection. DOJ Registrars collect fingerprints and a digital photograph of the applicant and transmit an enrollment package to the IDMS using the enrollment workstations.

4.4 Privacy Impact Analysis: Given the internal sharing, discuss what privacy risks were identified and how they were mitigated.

The privacy risk is that private information could be compromised by any of the roles filled by DOJ personnel. The risk is mitigated by having trained, vetted personnel fill these roles. All access for DOJ personnel to the GSA Managed Service system is role based, and requires a PIV card to log in. Personnel must be appointed and undergo training, including their responsibilities to protect privacy information. DOJ receives periodic reports which detail card issuances, revocations, and other information on card statistics. These reports are reviewed by Security and Emergency Planning Staff.

Section 5.0 External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to DOJ which includes foreign, Federal, state and local government, and the private sector.

5.1 With which external (non-DOJ) recipient(s) is the information shared?

The information is shared with GSA as the outsourced provider of PIV cards. Specifically, GSA will fill the following roles:

PIV Issuer (GSA Managed Service)**:** 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 Sponsor completes a PIV request for an applicant and submits it to the PIV Registrar and PIV Issuer. The PIV Registrar makes available following information to the PIV Issuer using the enrollment workstation:

- Facial image

- Copy of result of background investigation
- Other data associated with applicant (e.g. employee affiliation)

PIV Digital Signatory (GSA Managed Service): The entity that digitally signs the PIV biometrics and CHUID. This role applies for PIV-II. The PIV Registrar makes available to the PIV Digital Signatory:

- Electronic biometric data for card personalization
- Other data associated with the applicant that is required for generating signed objects for card personalization.

PIV Authentication Certification Authority (CA): The CA that signs and issues the PIV Authentication Certificate. This role applies to PIV-II

During the up-front background investigation process and identity proofing, relevant personal data will also be shared with the Office of Personnel Management (OPM), which is responsible for conducting the NACI and other higher-level investigations for DOJ.

Additionally, information about individuals that is stored for purposes of issuing a PIV card 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;
- 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 with complete description of routine uses was published in the Federal Register: GSA GOVT-7, Federal Personal Identity Verification Identity Management System (PIV IDMS), 71 FR 56983 (September 28, 2006).

5.2 What information is shared and for what purpose?

As described in 5.1 above.

5.3 How is the information transmitted or disclosed?

The information is transmitted electronically over encrypted VPNs from the enrollment station to the IDMS. Sponsorship information is sent by DOJ Sponsors using an encrypted web session. Sponsorship data for bulk uploads may be prepared using desktop office automation software, such as spreadsheets, or a custom software tool developed to format sponsorship data and produce a bulk upload file. The sponsorship software tool helps ensure the data is in the correct format prior to sending it to the GSA managed service system, reducing the risk of sending erroneous data. The bulk upload file is sent to the GSA managed service by a Security Officer over an encrypted connection. The completed PIV cards are mailed to DOJ.

5.4 Are there any agreements concerning the security and privacy of the data once it is shared?

Yes, the DOJ and GSA have signed a Memorandum of Understanding for DOJ to obtain PIV card services from GSA. There is an Interconnection Security Agreement describing data security and the responsibilities of GSA and DOJ for protecting the data.

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

All outside personnel undergo background investigations and must complete training to ensure they are knowledgeable about how to protect personally identifiable information. The training is accomplished by self-paced, web based learning modules which include an audio track, video clips, and screen shots.

5.6 Are there any provisions in place for auditing the recipients' use of the information?

Yes. GSA maintains an audit trail and performs random periodic reviews to detect unauthorized access or suspicious behavior. The periodic reports on card issuance activity are reviewed by DOJ. DOJ Sponsors and the Security Officer can view information on DOJ personnel in the GSA system.

5.7 Privacy Impact Analysis: Given the external sharing, what privacy risks were identified and describe how they were mitigated.

The risks to privacy data from sending DOJ data to an external agency were considered in the decision to outsource PIV card services to GSA. There is the risk that data could be compromised by either an internal or external actor. The risk is mitigated by multiple technical, physical, and administrative controls. The GSA system must meet all Federal Information Security Management Act requirements, as well as OMB and NIST policies and standards. DOJ will conduct a careful review of the certification and accreditation activities performed by GSA prior to using the system for any DOJ data.

Access to data is restricted by agency. Only DOJ appointed roles have access to DOJ data, with the exception of GSA database administrators and system administrators

who have access to data from all agencies using the GSA managed service. All outside personnel undergo background investigations and must complete training to ensure they are knowledgeable about how to protect personally identifiable information. An Interagency Agreement and Interconnection Security Agreement define DOJ and GSA responsibilities to protect data.

Section 6.0 Notice

The following questions are directed at notice to the individual of the scope of information collected, the opportunity to consent to uses of said information, and the opportunity to decline to provide information.

6.1 Was any form of notice provided to the individual prior to collection of information? If yes, please provide a copy of the notice as an appendix. (A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register Notice.) If notice was not provided, why not?

The System of Records Notice is attached as an appendix. The PIV Card Usage Privacy Act Notice is attached as an appendix.

6.2 Do individuals have an opportunity and/or right to decline to provide information?

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 or employment prospects.

6.3 Do individuals have an opportunity to consent to particular uses of the information, and if so, what is the procedure by which an individual would provide such consent?

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

6.4 Privacy Impact Analysis: Given the notice provided to individuals above, describe what privacy risks were identified and how you mitigated them.

Privacy concerns of individuals are mitigated by explaining the privacy implications of the PIV card system. The SORN and PIV Card Usage Privacy Act Notice are clearly written and available to all DOJ personnel.

Section 7.0 Individual Access and Redress

The following questions concern an individual's ability to ensure the accuracy of the information collected about him/her.

7.1 What are the procedures which allow individuals the opportunity to seek access to or redress of their own information?

Procedures to seek access to or redress their own information are specified in the SORN.

7.2 How are individuals notified of the procedures for seeking access to or amendment of their information?

The SORN was published in the Federal Register to provide this information.

7.3 If no opportunity to seek amendment is provided, are any other redress alternatives available to the individual?

Not Applicable.

7.4 Privacy Impact Analysis: Discuss any opportunities or procedures by which an individual can contest information contained in this system or actions taken as a result of agency reliance on information in the system.

The procedures are as described in the SORN. Additionally, the applicant may contact the PIV Card Applicant Representative.

Section 8.0 Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

8.1 Which user group(s) will have access to the system?

The roles described in 4.1 will have access to the system: PIV Sponsor, Registrar, Adjudicator, Security Officer. GSA database administrators and system administrators will have access to the data.

8.2 Will contractors to the Department have access to the system? If so, please submit a copy of the contract describing their role with this PIA.

No. However, contractors to the GSA managed service office will have access to the system.

8.3 Does the system use "roles" to assign privileges to users of the system?

Yes, as described in 4.1.

8.4 What procedures are in place to determine which users may access the system and are they documented?

All users filling roles on the system are appointed and must undergo training. They must possess a PIV card and use it to access the system. Access procedures are documented in the System Security Plan.

8.5 How are the actual assignments of roles and rules verified according to established security and auditing procedures?

The DOJ PIV issuance process must undergo a certification and accreditation in accordance with NIST Special Publication 800-79, which includes assignment of roles for the system. All access to the system is controlled through smart card login with the PIV card.

8.6 What auditing measures and technical safeguards are in place to prevent misuse of data?

Audit logs are maintained and reviewed periodically to detect unauthorized access. Enrollment packages are digitally signed to prevent data tampering. Data is segregated by agency, and users cannot access data from other agencies. No enrollment data is stored at or by the enrollment workstation or center. The enrollment record can only be viewed or retrieved by a DOJ 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, using the PIV card, which ensures only those with a need to access the data and who possess proper training can retrieve or view enrollment information.

8.7 Describe what privacy training is provided to users either generally or specifically relevant to the functionality of the program or system?

All users must undergo web based or instructor led training, which includes training to protect privacy data. Users also receive annual privacy training as part of computer security awareness training.

8.8 Is the data secured in accordance with FISMA requirements? If yes, when was Certification & Accreditation last completed?

Yes. Certification and accreditation of the GSA managed service system was completed in August 2007. Sponsorship data within DOJ is prepared for bulk upload using certified and accredited General Support Systems within DOJ components.

8.9 Privacy Impact Analysis: Given access and security controls, what privacy risks were identified and describe how they were mitigated.

The privacy risk identified was compromise of privacy data due to internal or external actors. Multiple technical, physical, and administrative controls are in place to mitigate the risk, as follows.

- GSA and DOJ assure that systems containing information in identifiable form (IFF) for the purpose of enabling the implementation of PIV are handled in full compliance with the Privacy Act.
- GSA and DOJ ensure that only personnel with a legitimate need for access to IIF are authorized to access the IIF, including but not limited to information and databases maintained for registration and credential issuance.
- GSA has categorized the system risk level (as specified in FIPS 199) and utilizes security controls described in NIST SP800-53, Recommend Security Controls for Federal Information Systems, to accomplish privacy goals, where applicable.
- The controls include network security and limited access to system and physical facilities.
- Controls include protecting data through the use of FIPS validated cryptographic algorithms in transit, processing and at rest.
- 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 “eavesdropping” is not allowed and that data is sent only to its intended destination and to an authorized user, by an authorized user.
- 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.
- 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.

- 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.

Security of the ID credential issued to an employee or contractor is achieved by full compliance with the mandatory requirements of FIPS 201. Specific safeguards include:

- Card issuing authority is 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.
- Sensitive card data is encrypted and stored on the card.
- Card is sheathed in electromagnetically opaque sleeve to protect against unauthorized contactless access to stored information.
- Employees are alerted to importance of protecting the card.
- Card expiration date is within 5 years from issuance.
- Return of cards to agency when no longer needed (or upon employee/contractor separation from the agency).
- Deactivation of card in case of employee/contractor separation, loss of card, or expiration.
- Removal of all IIF associated with the cardholder from the system upon deactivation if the cardholder will not be reissued a new card.
- Specialized role-based training for all persons involved in the PIV process.

Section 9.0 Technology

The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware, RFID, biometrics and other technology.

9.1 Were competing technologies evaluated to assess and compare their ability to effectively achieve system goals?

NIST analyzed all requirements of HSPD-12 and developed FIPS 201 as the appropriate solution to meet security, tamper-resistance, electronic authentication, interoperability, and privacy requirements.

DOJ and GSA must comply with the requirements specified in FIPS 201.

9.2 Describe how data integrity, privacy, and security were analyzed as part of the decisions made for your system.

All requirements derived from FISMA, NIST Special Publication 800-53, FIPS 201 and the NIST special publications developed to support FIPS 201 such as SP 800-73, SP 800-78, SP 800-76, and SP 800-79 were considered and incorporated into the system design.

9.3 What design choices were made to enhance privacy?

Only the minimum information necessary is collected. Encryption is used to send digitally signed enrollment packages through a virtual private network to the GSA IDMS. Access control is enforced by PIV cards. Physical security and administrative mechanisms were designed into the system to protect the information.

Conclusion

DOJ is meeting the activities and scheduled milestones required by HSPD-12 by utilizing an outsourced provider (GSA) for PIV card services. The GSA Managed Service system meets all Federal, OMB, and NIST standards and guidance for system security and protection of privacy data. All prudent security mechanisms are included in the system design to mitigate the risks of unauthorized exposure of DOJ data as much as possible.

Responsible Officials

John Murray, Director, Enterprise Solutions Staff

Scott K. Morrison, Information System Security Officer