U.S. Department of Housing and Urban Development

PRIVACY IMPACT ASSESSMENT FOR:

"PERSONAL IDENTITY VERIFICATION (PIV) PROCESS TECHNOLOGY AND DATABASE" IN COMPLIANCE WITH HOMELAND SECURITY PRESIDENTIAL DIRECTIVE 12 (HSPD-12)"

DECEMBER 2006

Document Endorsement

I have carefully assessed the Privacy Impact Assessment (PIA) for the "Personal Identity Verification (PIV) Process Technology and Database. This document has been completed in accordance with the requirement set for by the Privacy Act of 1974, E-Government Act of 2002, Homeland Security Presidential Directive 12 (HSPD-12), Federal Information processing Standard (FIPS) 201: Policy for a Common Identification Standard for Federal Employees and Contractors.

ENDORSEMENT SECTION

PLEASE CHECK THE APPROPRIATE STATEMENT.

X **THE DOCUMENT IS ACCEPTED.**

_____ **THE DOCUMENT IS ACCEPTED PENDING THE CHANGES NOTED.**

_____ **THE DOCUMENT IS NOT ACCEPTED.**

Based on our authority and judgment, the data captured in this document is current and accurate.

/s/ Ronald J. Salazar	**3/20/07**
Ronald J. Salazar , System Manager **Office of Administration, Office of Security and Emergency Planning**	**Date**
/s/ Robert E. Langston	2/1/07
Robert E. Langston, Program Area Manager **Ofice of Administration, Office of Security and Emergency Planning**	**Date**
/s/ Jeanette Smith	3/26/07
Jeanette Smith, Departmental Privacy Act Officer **Office of the Chief Information Officer**	**Date**

PRIVACY IMPACT ASSESSMENT FOR:
"PERSONAL IDENTITY VERIFICATION (PIV) PROCESS TECHNOLOGY AND DATABASE"
IN COMPLIANCE WITH HOMELAND SECURITY PRESIDENTIAL DIRECTIVE 12 (HSPD-12)"
updated December 2006

PIV Program PIA Reference Sheet

Unique Project Identifier Number (UPI): N/A
If no UPI, please explain why: Part of the Working Capital Fund (WCF) Infrastructure -- not a separate Exhibit 300
Systems of Records (SORs) Number: FR-4922-N-21/FR-4922-N-22
SOR Title: Identity Management System/Personnel Security Files

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

IT Security Plan Number(s): Will be completed by June 2007
IT Security Plan Title: Will be completed by June 2007
Accreditation and Certification Date: Will be completed by June 2007

OMB Exhibit 300 Number: N/A (part of the IT Working Capital Fund (WCF) "infrastructure" project
OMB Exhibit 300 Title: N/A (part of the IT Working Capital Fund (WCF) "infrastructure" project

Identity Proofing and Registration Process Approval Date: PIV-I Guide issued Oct. 26, 2005

PIV Implementation Plan Approval Date:

Contact Name, Title: Sandy Timbrook, Director, Security Division
E-Mail: Sandra_L._Timbrook@HUD.gov
Organization/Department: Office of Administration, Office of Security and Emergency Planning, HUD
Phone Number: (202) 708-4022 ext. 7301

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

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. See the Presidential Directive at http://www.whitehouse.gov/news/releases/2004/08/20040827-8.html. See Office of Management and Budget (OMB) implementing policy guidance on HSPD-12 at http://www.whitehouse.gov/omb/memoranda/fy2005/m05-24.pdf. See OMB guidance on privacy as related to HSPD-12 at http://www.whitehouse.gov/omb/memoranda/fy2006/m06-06.pdf and sample documents (which was the basis for this document) at http://www.whitehouse.gov/omb/memoranda/fy2006/m06-06_att.doc.

HSPD-12 requires that the Federal credential be secure and reliable. The credential is for physical access (to buildings and office space), as well as "logical" access (to computer networks and applications). 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. See FIPS 201 and related NIST Special Publications at NIST's PIV web site at http://csrc.nist.gov/piv-program/.

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 ("smart cards") for access to Federal facilities and Federal information systems. 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.

In response to HSPD-12 and to meet the requirements summarized above, ***HUD's* Office of Security and Emergency Planning (OSEP)** is responsible for the identity management and all aspects of the HUD 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 Field Administrative Service Centers (ASCs) and selected Field Administration staff have been granted "authorization to operate" as certified PIV Registrars. HUD is currently expecting to issue approximately **12,000** PIV-II standard ID badges/ smartcards for building and computer access at HUD Headquarters and in the 81 Field Offices between October 2006 and October 2008 – covering all employees and contractors Department-wide..

Privacy Impact Assessment (PIA) Scope

This PIA provides details about HUD'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 the standardized and secure processes required for personal identity verification (PIV) 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), which is the database used for identity management and access control; and (iv) the PIV card itself.

As noted previously, PIV-I requires the implementation of registration, identity proofing, and issuance procedures compliant with the standards of FIPS 201. See http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf. However, the collection of information for background investigations has been a long-standing requirement for Federal employment. This process and the data elements used are not new. The forms and information collection for the background investigation process will continue to occur as they have for many years throughout the Federal Government. Additionally, PIV-I may not require the implementation of any new systems or technology. HUD will continue to issue ID badges, 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. These processes will be referred to throughout this PIA as theHUD PIV program, and the credentials (ID badges) issued will be referred to as PIV cards.

Basic Program Control Elements

There are four "control objectives" of the PIV program, as defined in the Presidential Directive (HSPD-12):

> "'Secure and reliable forms of identification' for purposes of this directive means identification that (a) is issued based on sound criteria for verifying an individual employee's identity; (b) is strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation: (c) can be rapidly authenticated electronically; and (d) is issued only by providers whose reliability has been established by an official accreditation process." See 3rd paragraph of HSPD-12 at http://www.whitehouse.gov/news/releases/2004/08/20040827-8.html.

As stated in FIPS 201 (section 2.1), each agency's PIV implementation must meet the four control objects, such that:

- Credentials are 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 issued picture ID.
- 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.
- No credential is issued unless requested by a proper sponsor.
- A credential remains serviceable only up to its expiration date. More precisely, 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 not modified, duplicated, or forged.

See http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf (section 2.1).

SECTION 1.0 INFORMATION COLLECTED AND USED IN THE PIV PROGRAM

1.1 What information is collected and from whom?

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 hire, either a Federal employee or a contractor. As required by FIPS 201, **HUD** will collect biographic and biometric information from the PIV Applicant in order to: (i) conduct the background investigation or other national security 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 processes.

For HUD's Field staff, they receive PIV Enrollment and PIV Card Issuance services through the Government-wide HSPD-12 Shared Services solution, managed by the General Services Administration (GSA). GSA has published a PIA for their portion of the PIV enrollment and PIV Card issuance process. That Government-wide PIA is incorporated by reference into this HUD-specific PIA.

Figure 1: The Collection, Storage and Use of Information from the PIV Applicant

	Background Investigation	Identity Proofing and Registration	IDMS (Electronically Stored)	PIV Card (Physically Displayed)	PIV Card (Electronically Stored)
Date of birth	X	X	X		
Place of birth	X	X	X		
Social Security Number (SSN)	X	X	X		
Other names used	X	X	X		
Citizenship	X	X	X	Blue Stripe for foreign national	X
Other identifying information (height, weight, hair color, eye color, gender)	X	X	X	Optional	Optional
Organizational affiliation (e.g. Agency name)	X	X	X	X	X
Employee affiliation (e.g. Employee or contractor)	X	X	X	X	X

	Background Investigation	Identity Proofing and Registration	IDMS (Electronically Stored)	PIV Card (Physically Displayed)	PIV Card (Electronically Stored)
Fingerprints (10)	X	X	X		
Biometric identifiers (2 fingerprints digitally converted to "key points" minutiae templates)		X	X	Not visible	Stored as "key points" (not full image of fingerprints)
Digital color photograph (captured by Registrar)		X	X	X	X
Digital signature [1]			X		X
Telephone numbers	X	X	X		
Spouse (current or former), relatives and associates, information regarding their citizenship	X				
Marital status	X				
Employment history	X				
Address history	X		X[2]		
Educational history	X				
Personal references	X				
Military history/record	X				
Illegal drug history	X				
Criminal history	X				
Foreign countries visited	X				
Background investigations history	X				
Financial history	X				
Association history	X				
Signed PIV Request		X	X		
Signed SF-85 or SF-85P or SF-86	X		X		
Copies of identity source documents		X	X		

1.2 What is the information used for?

[1] Public key infrastructure (PKI) digital certificate with an asymmetric key pair. The PKI digital signature certificate is an optional feature, to be used for "signing" computer transactions.

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

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

1. **Conduct a background investigation.** A Federal background investigation including "National Agency checks" has been a condition of Federal employment (including consultants and contractors) since President Eisenhower signed Executive Order 10450 in April 1953. Many subsequent Executive Orders have reaffirmed and clarified or expanded the requirements for Federal background investigations. Also, there is an extensive set of regulations and policy issued by the Office of Personnel Management (OPM) which gives guidance to agencies on the process for conducting background investigations and adjudicating the results. FIPS 201, issued in April 2005, reaffirms and incorporates these long-standing requirements for background investigations, as related to identity proofing and credential issuance. Before a PIV Card (the new Federal-wide ID badge/ smart card) can be issued, specific background investigation related requirements must be met. Specifically, a PIV Applicant must either already have a completed background investigation, or if none has been done, then (1) the National Agency Check with Written Inquiries (NACI) must be initiated, and the FBI National Criminal History (Fingerprint) Check must come back "favorable" (indicating lack of criminal history). When these conditions are met, then agencies are allowed to issue the PIV Card. Doing the FBI Fingerprint Check matches a PIV Applicant's 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). A Government-wide form is used to initiate the background investigation, depending on the sensitivity of the position and sensitivity of systems access. The minimum background investigation is the NACI, and this is initiated by the PIV Applicant filling out a Standard Form 85, Questionnaire for Non-Sensitive Positions. For sensitive positions or sensitive systems access, the PIV Applicant fills out Standard Form 85P, Questionnaire for Positions of Trust, which results in a higher level of background investigation. Those in positions requiring a National Security Clearance (secret or top secret) fill out Standard Form 86, Questionnaire for National Security Positions..[3] The background investigation process entails conducting a National Agency Check with Written Inquires (NACI), which includes 4 database checks, plus written inquiries, as described below:

   - **National Agency Checks (NACs):** Consists of searches of (1) the OPM Security/Suitability Investigations Index (SII), (2) the Defense Clearance and Investigations Index (DCII), (3) the Federal Bureau of Investigation (FBI) Identification Division's name files (FBI Name Check), and (4) the FBI National Criminal History (Fingerprint) Check, and other files or indices when necessary.

[3] SF 85, SF-85P, and SF 86 can be downloaded at: http://www.opm.gov/forms/html/sf.asp

- **Written Inquiries:** Form letters are sent to former employers and to those who can verify the PIV Applicant's residence over the past 5 years (for a NACI), or 7 years (for a higher background investigation), or a longer period (for National Security Clearances).

Note: The background information collected as part of this process and its results are kept in the background investigation files; however, none of this information is stored on the PIV Card.

2. **Complete the identity proofing and registration process.** The biographic information (name, etc.) collected as part of this process is used to establish the PIV Applicant's identity. Biometrics (fingerprints and photo) are used to ensure PIV Applicants have not been previously enrolled in the PIV system. As part of this process, FIPS 201 requires that PIV Applicants provide two 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.[4] PIV Applicants sign for the resulting PIV Card, confirming that they have received and understand the the Privacy Act Statement associated with the PIV Registration and PIV Card issuance process. By signing the SF-85, SF-85P, or SF-86 (in item 1 above), they also agree to have their personal information used as part of the OPM-conducted background investigation. Headquarters employees and contractors will be processed at the Office of Security and Emergency Planning (OSEP). Field staff will be processed through shared enrollment stations being set up in about 200 key cities across the country. These shared enrollment stations are managed by the General Services Administration (GSA), and supported by the U.S. Department of Agricultue (USDA) and the U.S. Department of Interior. Agencies like HUD who have signed up to use the "HSPD-12 Shared Services Solution" on a fee-for-service basis send employees and contractors to be registered at the shared enrollment stations, and to get a PIV Card.

3. **Create a data record in the PIV Identity Management System (IDMS).** The IDMS is a computer application and database used during the PIV registration process. Itcreates the PIV Applicant's enrollment record, manages and maintains this information throughout the PIV card lifecycle. The IDMS is also used in conjunction with the Card Management System (CMS) and the physical access control system (PACS) to verify, authenticate, and revoke PIV cardholder access to federal facilities (buildings and office space). Likewise, the IDMS is the key data source for verifying identity when PIV Cardholders seek "logical" access to Federal information systems (using the electronic authentication features of the combination ID badge/ smart card). A Card Holder Unique Identifier (CHUID) is assigned during registration, and is used to represent the individual's identity and associated attributes stored in the system. This is a unique number that distinguishes each PIV Card from another, across the entire Federal Government. It is comprised of the 4-digit agency code (such as 8600 for HUD), plus a

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

sequential number for each person at that agency reciving a PIV Card (8600-0001, 8600-0002, etc.). The CHUID does not contain personal information such as Social Security Number, but rather uses a "non-personal" unique identifier as described, similar to being a "serial number." For HUD Headquarters staff, this data is stored in HUD's own IDMS. For HUD Field staff, the initial capturing of enrollment data is in the GSA/ USDA/ Interior IDMS. After the PIV Card is produced, the enrollment data is securely transferred from the Shared Services IDMS to HUD's IDMS, and the data is then deleted from the Shared Services IDMS.

4. **Issue a PIV card.** A PIV card is issued upon successful completion of (1) the FBI National Criminal History Fingerprint Check portion of the NACI background investigation (with "favorable" results); (2) identity proofing with 2 acceptable identity source documents; and, (3) successful completion of the registration/ enrollment process. Biometrics (index fingerprints) are used during PIV Card issuance to verify PIV Applicant identity and complete activation of the PIV 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. As described above, HUD Field staff are sent to the shared enrollment stations. The PIV Cards for the Field staff will be produced by the Shared Services Solution managed by GSA.
5. **Usage of PIV Card for physical and logical access:** On a routine basis, the electronic authentication features built into the PIV Card will be sufficient to gain physical access to facilities (buildings and office space). However, the PIV Card standards allow for "graduated levels of security" and multiple methods of authentication. For higher security areas or more sensitive computer systems, the advanced features of the PIV Card may optionally be used. At the highest levels of security access, the index fingerprint "key points" may be required, to verify that the person holding that PIV Card is in fact the same person to whom it was issued (using "biometric match" technology). The biographic and other information displayed on the PIV Card (name, agency, expiration date, etc.) is used by physical security guards for identity verification purposes. The PIV Card may be used for either visual inspection, or for electronic verification through a compliant PIV Card reader.

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

Additionally, the IDMS and the 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 are described in Figure 2.

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 to allow access to Federal facilities and computer systems
Personal Identification Number (PIN) – 6 digits, selected by the Card holder and programmed into the PIV Card, similar to a bank automated teller machine (ATM) card			X	For optional/ selected use either for physical access to highly secured buildings/ space or to log-on to sensitive computer systems that require multi-factor authentication ("level 3" assurance of identity), beyond the typical user ID/ password.
Agency card serial number – unique for each card	X	X	X	For identifying and maintaining agency cards
Issuer identification number	X	X	X	To verify issuer's authority to issue PIV Cards
"Contact" Integrated Circuit Chip (ICC) – for inserting the PIV Card into a "contact" card reader			X	Used to authenticate a PIV cardholder's identity with card readers that require card to be inserted. Can be used for physical access to buildings/office space and logical access to computer systems.
"Contactless" ICC – for "swiping" the PIV Card near a "contactless" (radio frequency) card reader			X	Used to authenticate a PIV cardholder's identity with low-frequency radio signal card readers that allow card to pass by the card reader (within about 5 centimeters), if the radio frequency sent by the PIV Card's "antenna" matches that of the card reader. Primary use is for physical access to buildings and office space where a card reader controls access.
PIV authentication keys	X		X	Used to authenticate the PIV card to the card reader and the physical access control system in order to validate a PIV cardholder's identity prior to granting access.
Cardholder Unique Identifier (CHUID), which includes the Federal Agency Smart Card Credential Number (FASC-N)	X		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

	IDMS (Electronically Stored)	PIV Card (Physically Displayed)	PIV Card (Electronically Stored)	Purpose
				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 identity and authority of the individual (Registrar) who identity-proofed the PIV Applicant and approved him/her to get a PIV Card. Also used to certify that the enrollment record is complete and approved by the PIV Registrar.

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

No "commercial databases or data" are used in the PIV process. However, agencies do have an automated link to OPM's Personnel Investigations Processing System (PIPS). PIPS allows agency Personnel Security Officers and others specifically delegated to check on prior background investigations (NACI or higher). If the PIV Applicant has had a prior background investigation that is sufficient for their current duties and systems access, then they can be issued a PIV Card without initiating a new background investigation. PIPS is government-controlled information, and not "commercial."

1.5 (a) Will new or previously unavailable information about an individual be obtained or generated? (b) If so, what will be done with the newly derived information? (c) Will it be placed in the individual's existing record? (d) Will it be placed in an existing system of records? Will a new system of records be created? (e) 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.

(a) The new PIV process requires capturing the full 10 fingerprints in electronic form and storing them in an identity management system (IDMS). The 2 index fingerprints are also stored on the PIV Card, but as "minutiae templates" – meaning a mathematically derived file that distinguishes the key points of the fingerprint pattern. All other personally identifiable information that is collected is the same as the previous process (such as that collected on the SF-85, SF-85P, or SF-86) has been in place government-wide for decades.

(b) The "minutiae template" index fingerprints are optionally used for access to more secure facilities or information systems. They will not be required on a routine basis in all agencies. When required, they verify that the person using the PIV Card is the same person whose "minutiae template" fingerprints are stored on that Card, with 99%+ accuracy. The full image of the 10 fingerprints are captured in electronic form and are used for the FBI National Criminal History Check, as part of the Federal background investigation. This requirement for national agency checks (NACs) has been in place for decades, with the authority cited as Executive Order 10450, signed by President Eisenhower in April 1953. One of the requirements of the new PIV process is that the FBI National Criminal History Check (based on comparing the individuals fingerprints with the FBI's database of arrest records) is found "favorable" prior to issuing the PIV Card. In other words, the person must either have no arrest record, or if there is an arrest record, the agency's "Adjudicator" (Personnel Security Officer) must determine that the person is suitable for Federal employment in the assigned position.

(c) Yes, the fingerprints (both the "minutiae templates" of the index fingerprints and the full image of the 10 fingerprints) are associated with the individual and become part of his/her record. The "minutiae templates" are one of the features that enables electronic authentication for access to Federal facilities or information systems. The 10-prints are part of the background investigation that determines the individual's identity as well as suitability for Federal employment (including working as a contractor).

(d) HUD recently published a Federal Register Privacy Act System of Records Notice (SORN) to cover the comprehensive Identity Management System (IDMS). It includes the fingerprint information described above.

(e) Yes. See (a), (b) and (c) above.

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

HUD collects only the type and amount of personally identifiable information as required of all Federal agencies in the Executive Branch. The background investigation information (primarily collected on the SF-85, SF-85P, or SF-86) is dictated by Office of Personnel Management (OPM) policy and regulations. The new PIV process is dictated by Federal Information Processing Standards 201 (FIPS 201). Rather than creating new requirements, FIPS 201 basically standardizes the procedures long-existent throughout the Federal Government for identity proofing and ID badging. The standardized process is strengthened by requiring at least two officials to approve and issue ID badges. Further, the process is strengthened by requiring the FBI National Criminal History Check to be favorable before the ID badge can be issued.

Because much of the PIV process has already been in place Government-wide, the privacy risks are not new, nor are the ways that agencies mitigate those risks. Specifically, these are the privacy risks and how HUD mitigates those risks:

- Risk: Information from the SF-85, SF-85P, or SF-86 forms could potentially get into the wrong hands, and "identity theft" could occur.
    - Mitigation: Only those who hold "positions of trust" (such as human resources specialists, administrative officers, personnel security officers, system security administrators, and PIV Registrars) are authorized to handle the background investigation and PIV forms. Restricting who can handle these documents greatly reduces the risk of potential identity theft of such information as full name, Social Security number, date of birth, place of birth, and home address.

- Risk: Personally identifiable information stored in the Identity Management System (IDMS) or personnel security databases could potentially be accessed by unauthorized persons.
    - Mitigation: These systems and databases are restricted to those in positions of trust. Systems are password protected. Authorized users have been trained on computer security rules, as well as the punishments and fines for deliberate or negligent violations of the Privacy Act. Those supervising the PIV Registrars monitor use of the systems and databases.
- Risk: Background investigation and PIV paper files could be seen or taken by unauthorized persons.
    - Mitigation: FIPS 201 requires that PIV forms be locked when not in use, and that every caution be taken to prevent unauthorized persons from seeing the files. OPM regulations require that the documents related to a person's criminal history be kept in "3-position combination lock safes" – to ensure the greatest confidentiality of these highly sensitive records. Only the agency's OPM-certified adjudicators (personnel security officers) are authorized to see the details of an individual's criminal history records.

SECTION 2.0 INTERNAL SHARING AND DISCLOSURE

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

The information is shared with authorized HUD employees and a limited number of trusted contractors who are directly involved in the design, development, implementation and execution of HUD's PIV program who, by law and contract, are bound by the Privacy Act. Specific information about a PIV Applicant or Cardholder will be shared with HUD employees who have a "need to know" for implementation of the PIV Program. Trusted HUD contractors are contractually obligated to comply with the Privacy Act in the handling, use, and dissemination of all personal information.

The critical roles are PIV identity proofing, registration, and card issuance processes are described below, as described in FIPS 201. All individuals are trained and certified (tested) to perform his or her respective role; however, these roles are often ancillary roles assigned to personnel who have other primary duties.

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 the Bureau, Organization or Regional Office 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 the Bureau, Organization or Regional Office; and (iv) have 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 Card Issuer. The PIV Request includes the following information:

- Name, organization, and contact information of the PIV Sponsor, including the address of the sponsoring organization
- Signature of the PIV Sponsor.
- Name, date of birth, position, and contact information of the Applicant
- Name and contact information of the designated PIV Registrar
- Name and contact information of the designated PIV Issuer

2. **PIV Registrar:** The entity (person or organization) 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 can 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, SF-85P, or SF-86 (as required for the position)
   - Two identity source documents in original form

   The PIV Registrar will record the following data for (or make a copy of) each of the two identity source documents, sign the records, and keep it on file:
   - document title
   - 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 the Applicant, and retains a file copy of the image.
- Fingerprints the Applicant, obtaining all fingerprints, and retains a copy.
- Initiates a Federal background investigation, or verifies with proper authorities that a prior Federal background investigation at an acceptable level was already conducted. As a minimum, the National Agency Check with Written Inquiries (NACI) must either be initiated or on file. For those in "positions of trust" or requiring access to sensitive computer systems, a background investigation higher than a NACI will be required (using the SF-85P or SF-86 instead of the SF-85). If a prior Federal background investigation has not been previously conducted (or if it cannot be verified), then a new one must be initiated. The portion of the background investigation known as the FBI National Criminal History (Fingerprint) Check must be completed and found "favorable" prior to issuing the PIV Card.
- Notifies the sponsor and designated PIV Card Issuer that the Applicant had been approved for a PIV Card (or not).

3. **PIV Card Issuer:** 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 the following information to the PIV Card Issuer:
   - Facial image copy of result of background investigation
   - Other limited data associated with applicant (e.g. employee affiliation)

   The PIV Card Issuer does <u>not have access to the information on the SF-85, SF-85P, or SF-86 because the PIV Card Issuer does not have a need to know this personally sensitive information.</u>

4. **PIV Digital Signatory:** The entity (person or organization) that digitally signs the digital certificates, digitized biometrics, and the Card Holder Unique Identifier (CHUID). The PIV Registrar makes available to the PIV Digital Signatory:
   - Electronic biometric data ("minutiae templates" of the two index fingerprints) for card personalization
   - Other limited data associated with the Applicant that is required for generating signed objects for card personalization.

5. **PIV Authentication Certification Authority (CA):** The CA that signs and issues the PIV Authentication Certificate. The PIV Card has a mandatory digital certificate that can be used for authentication between the PIV Card and a PIV Card reader

for physical access control systems (PACS). The PIV Card also has optional digital certificates that can be used for authentication to computers for logical access control systems (LACS).

6. **PIV Adjudicator:** [Note: According to NIST standards, the PIV Adjudicator may perform the role of the PIV Registrar.] The PIV Adjudicator is the entity (organization or individual) responsible for determining whether the Applicant is suitable to receive a PIV 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 a "Certificate of Investigation."

7. **Enrollment Official:** [Note: According to NIST standards, the Enrollment Official may perform the role of the PIV Registrar.] The Enrollment Official is responsible for performing identify-proofing for applicants at locations that do not have a PIV Card Issuing Facility, Registrar, or Servicing Human Resources Office. The Enrollment Official verifies the claimed identity of the applicant, creates the registration package to be submitted to the Registrar, and issues the personalized PIV credential to the applicant.

8. **PIV Card Issuing Facility (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 FIPS 201 requirements.

9. **System Administrator:** The System Administrator manages the Identity Management System (IDMS) and controls who has access to the system and its data.

SECTION 3.0 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 Office of Personnel Management (OPM) who is responsible for conducting the NACI and other higher-level background investigations for HUD and

2. 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.

Additionally, information about individuals that is stored for purposes of issuing a PIV card and to run the HUD PIV program may be given without individual's consent as permitted by the standard disclosure provisions of 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;
- a limited number of agency contractors who are specifically authorized to have access to the records to do agency work and who have agreed to comply with the Privacy Act;
- the National Archives and Records Administration (NARA) for records management inspections; and
- other federal agencies to notify them when a PIV card is no longer valid, or has been revoked.

The full system of records notice (SORN) with complete description of routine uses was published in the Federal Register at FR-4922-N-21/ FR-4922-N-22and can be viewed at: http://frwebgate2.access.gpo.gov/cgi-bin/waisgate.cgi?WAISdocID=705361375708+0+0+0&WAISaction=retrieve/ http://frwebgate5.access.gpo.gov/cgi-bin/waisgate.cgi?WAISdocID=705435140677+0+0+0&WAISaction=retrieve

3.2 Is HUD either providing or receiving card issuance services pursuant to a serving agreement? [*If yes for either case, describe the privacy implications of the servicing agreement (including the transmission, storing, and maintenance of data), and how each agency will address the potential privacy risks.*] Reference GSA's PIA for shared enrollment services.

SECTION 4.0 AGENCY POLICY REQUIREMENTS

[*Identify any existing department or agency policies that relate to or apply to this program (i.e. policy on unauthorized browsing, labeling/handling of sensitive data, etc.).*]

SECTION 5.0 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 notices required by the Privacy Act, 5 USC 552(a)(e)(3). The notice(s) state(s) 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 complies with the Privacy Act and the published System of Records Notice(s) (SORN) for the Personnel Security Files and the Identity Management System.. A copy of the Privacy Act Notice is attached.

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

5.2.1 Cite any procedures or regulations in place that allow access to information according to FOIA/Privacy Act regulations. Agencies that have customer satisfaction units should provide phone and email information in addition to specific FOIA/Privacy Act procedures. 24 CFR Part 16, Handbook 1325.01 REV-01

5.2.2 If the system is exempt from the amendment/correction provisions of the Privacy Act, please explain the basis for the exemption or cite the source where this explanation may be found (i.e., the exemption rulemaking published in the Federal Register). The system is not exempt from the amendment/correction provisions of the Privacy Act.

5.3 What are the procedures for correcting information?

5.3.1 Discuss the procedures and provide contact information for the appropriate person to whom such issues should be addressed. [*Cite information from agency Privacy Act regulation*.] 24 CFR 16.8, Procedures for correction or amendment to a record. Any individual, regardless of age, may submit to the Department a request for correction or amendment of a record pertaining to that individual. The request should be made either in person at the Office of, or by mail addressed to: the Privacy Act Officer, in the Office of the Chief Information Officer. Although an oral request may be honored, a requester may be asked to submit his or her request in writing. The envelope containing the request and the letter itself should both clearly indicate that the subject is a PRIVACY ACT REQUEST FOR CORRECTION OR AMENDMENT.

5.3.2 Describe how information collected from individuals or derived from the system is checked for accuracy. HUD maintains only information on individuals that is relevant and necessary to the performance of its lawful functions, to maintain that information with such accuracy, relevancy, timeliness and completeness as is reasonably necessary to

assure faireness in determinations made by the Department about the individual. Information is obtained directly from the individual to the extent practicable and reasonable to protect that information from unwarranted disclosure. The Department will maintain no information from unwarranted disclosure.

5.3.3 Describe any processes or procedures in place to reduce inaccuracies in data collected. Privacy Systems of Records Notices are published in the Federal Register to inform both the public and HUD employees of any personal information the Department collects about about them. Procedures are in place that allow individuals to review and correct any inaccuracies in the data collected.

5.4 How are individuals notified of the procedures for correcting their information? [*Describe.*] Individuals are notified of the procedures for correcting their information when System of Records Notices that contain information about them are published in the Federal Register.

5.5 If no opportunity to amend is provided, what alternatives are available to the individual? [*Describe.*] Individuals are provided an opportunity to amend their records.

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

While providing the information is voluntary, if individuals do not provide the requested information in whole or in part, we will not be able to complete their identity proofing and registration process. If an individual does not have a PIV card, they will be treated as a visitor when entering the HUD building. They will not have access to certain resources. If holding a PIV card is a condition of employment or obtaining a contract, failure to provide the requested information will adversely affect the individual's placement 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? No. Providing the information on the SF-85 etc. for the Federal background investigation is a condition of working for the Federal employment (as a Federal employee or contractor). None of the information is optional. By signing and submitting the SF-85 etc., the employee or contractor consents to using the information to conduct the Federal background investigation. The individual cannot "opt-out" of the use of the information.

5.8 What deficiencies in your agency procedures did you remedy after performing this analysis? We have re-emphasized to the PIV Registrars in both Headquarters and throughout the Field Offices of the need to keep personally identifiable information related to PIV securely stored/ locked when not being processed.

SECTION 6.0 DATA PROTECTION CONTROLS

6.1 General Program Controls

[*For your Agency describe whether and how you implement general program controls. Sample provided below.*]

- The organization has an approved identity proofing and registration process. This is fully described in HUD's Personal Identity Verification (PIV) Guide, issued to HUD Principal Staff and Regional Directors by the Deputy Secretary on Jan. 5, 2006.
- The applicant appears in-person at least once before the issuance of a PIV credential. The Applicant must appear before the PIV Registrar and show 2 forms of acceptable identification. Then, prior to issuance of the PIV Card, the Applicant must appear before the PIV Card Issuer and show a photo ID to confirm identity.
- 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. Yes, this requires the cooperation of the PIV Sponsor, PIV Registrar, and PIV Card Issuer.
- The identity proofing and registration process is accredited by the department or agency as satisfying the requirements and approved in writing by the head of the Federal department or agency. Yes. HUD's Deputy Secretary concurred on HUD's HSPD-12 Implementation Plan submitted to the Office of Management and Budget in June 2005, approving the PIV process. The Deputy Secretary also signed a memo to HUD Principal Staff and Regional Directors, transmitting HUD's 40-page PIV Guide. HUD's certification and accreditation (C&A) of the PIV process was conducted in November 2005 and updated in April 2006, approved by the Assistant Secretary for Administration as the Designated Accreditation Authority (DAA), as described by NIST Special Publication 800-79.
- The organization has an approved PIV credential issuance and maintenance process. Yes. See comments above.
- The organization issues PIV credentials only through systems and providers whose reliability has been established by the agency and so documented and approved in writing (i.e., accredited). Over 100 PIV Registrars have been trained and certified for their role, in compliance with HSPD-12 and FIPS 201 requirements. Annual re-certification and re-accreditation is conducted.
- A comprehensive privacy impact assessment (PIA) is conducted on systems containing personal information in identifiable (IIF) form for implementing PIV, consistent Section 208 of the E-Government Act and OMB Memorandum M-03-22. Yes. This document serves as the PIA for HUD's Identity Management System (IDMS) that supports the PIV process.
- The organization has generated a Federal Register system of records notice (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. Yes, a SORN for HUD's IDMS was published in October 2006. The full

system of records notice (SORN) with complete description of routine uses was published in the Federal Register at FR-4922-N-21/ FR-4922-N-22and can be viewed at: http://frwebgate2.access.gpo.gov/cgi-bin/waisgate.cgi?WAISdocID=705361375708+0+0+0&WAISaction=retrieve/ http://frwebgate5.access.gpo.gov/cgi-bin/waisgate.cgi?WAISdocID=705435140677+0+0+0&WAISaction=retrieve

- The organization assures that systems containing IIF for the purpose of enabling the implementation of PIV are handled in full compliance with the Privacy Act. Yes. See Section 1.5, Section 1.6, Section 3, and Section 5 above for details.
- The organization ensures 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. Yes. See Section 1.5, Section 1.6, Section 3, and Section 5 above for details.
- The organization coordinates with appropriate department or agency officials to define consequences for violating privacy policies of the PIV program. Consequences for violating privacy policies are outlined generally in HUD's Privacy Act Handbook.
- The organization assures that the technologies used in the department or agency's implementation of PIV data 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. "Continuous auditing of compliance with stated privacy policies and practices…" will be addressed – implemented in the future.
- The organization 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. A system security plan as well as a certification and accreditation (C&A) of the identity management system (IDMS) and card management system (CMS) will be prepared. These are in process (due by June 2007), led by the Office of the Chief Information Officer, with support from the Office of Security and Emergency Planning (OSEP).
- The organization ensures that the technologies used to implement PIV sustain and do not erode privacy protections relating to the use, collection, and disclosure of information in identifiable form. Specifically, employ an electromagnetically opaque sleeve or other technology to protect against any unauthorized contactless access to information stored on a PIV credential. HUD's implementation of the new Federal-wide PIV Card will meet all the standards in FIPS 201 and related NIST Special Publication 800-73. This includes the "electromagnetically opaque sleeve" which prevents hackers from being able to read data from the PIV card "in the clear" (secretly picking up data from the PIV Card without using the contact-chip and contactless chip technology).

6.2 Specific program controls used to secure information.

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

[*Note: This section assumes central card production and shared enrollment capabilities across agencies. Agencies may need to modify once final decisions on these work flow components are made. Privacy risks should include a discussion of system security and security of the PIV credential.*]

The agency follows all applicable government-wide standards for controlling and protecting information systems (see NIST Special Publication 800-53). Specific controls are described below. A system security plan as well as a certification and accreditation (C&A) of the identity management system (IDMS) and card management system (CMS) will be prepared. These are in process (due by June 2007), led by the Office of the Chief Information Officer, with support from the Office of Security and Emergency Planning (OSEP). These documents will cover the 8 areas below, as required by NIST Special Publication 800-53.

System security: [*Describe protections, e.g.*] The controls include network security and limited access to system and physical facilities. These risks are addressed by the IT Security Plan established for this PIV program and any associated IT Security Plan identified for each component of the PIV program listed in Section 7. More specific program controls include protecting data through the use of FIPS validated cryptographic algorithms in transit, processing, and at rest. See comment in 6.2, paragraph 1.

Networks: [*Describe protections, e.g.*] 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 "eavesdropping" is not allowed 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. Access is PIN protected. See comment in 6.2, paragraph 1.

Databases: [*Describe protections, and identify the administrative, operational and technical controls applied to protect this IDMS data repository containing biographical data, photo images and biometric identifiers.*] See comment in 6.2, paragraph 1.

Data Transmission: [*Describe protections, e.g.*] The 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, 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 handled 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) - 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 verificationSee comment on page 23, 6.2, paragraph 1.

Data Storage Facilities: [*Describe protections, e.g.*] 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). See comment on page 23, 6.2, paragraph 1

[*For central card production only: e.g.*] 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: [*Describe protections, e.g.*] User Identification: 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). See comment on page 23, 6.2, paragraph 1 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.
- Access Control: Access to data is PIN protected.

- 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.
- An Information Assurance and Security plan containing all technical measures and operational procedures consistent with federal law, FIPS 201, related Special Publications and agency policy.
- 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 [*agency*] and complete a training process associated with their specific role in the PIV process.

Separation of Duties Controls: [*Describe the roles of PIV Applicant, Sponsor, Registrar, PIV issuer and PIV Digital Signatory. Are the roles exclusively drawn? How does the agency ensure these roles do not overlap?*] See comment on page 23, 6.2, paragraph 1
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: See comment on page 23, 6.2, paragraph 1

- 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 contactless access to stored information
- Employees are alerted to importance of protecting card
- Card expiration 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 within 18 hours (the latest) of employee/contractor separation, loss of card, or expiration
- Removal of all IIF 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?

The PIV Registrars (fulfilling the roles prescribed by FIPS 201) are the primary staff with access to PIV information. The two full-time PIV Registrars at HUD Headquarters are in the Office of Security and Emergency Planning, working within secured office space. The 100+ part-time PIV Registrars in HUD's Field Offices are all in the Administrative Service Center (ASC) organizations. In the 10 Regional Offices, most of the PIV Registrars are Human Resources managers/ specialists or Administrative Officers. In the non-Regional Field Offices (about 45 locations having PIV Registrars), they are usually Administrative Officers or Administrative Specialists. All of these people are accustomed to handling personal information as part of their regular duties. The PIV Registrar role is an added function that is compatible with their other responsibilities as Human Resources or Administrative Services managers or staff.

In Headquarters only, HUD's Identity Management System (IDMS) and Card Management System (CMS) provide automation for the PIV process and the resulting ID badges. In the Field, the PIV process is paper-based as of December 2006. In Headquarters, authorized information technology (IT) personnel or contractors (pursuant to an appropriate routine use) who handle the operations and maintenance of the system 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, as allowed by the Privacy Act, HUD's Office of Inspector General (OIG) may request and be given access to the data, and HUD's General Counsel's Litigation Division may request and be given access to the data to represent HUD in litigation matters related to the PIV system. The described access by OIG and OGC is specifically authorized by section (b) (1) of the Privacy Act.

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

HUD's PIV Guide describes in detail the roles, responsibilities, and procedures for PIV processing, The PIV Guide covers privacy awareness and controls. Privacy is also a key subject in the training and resulting test of PIV Registrars, which are required prior to them being certified to perform the PIV Registrar role.

All assigned employees and assigned contractor staff receive privacy and security training. Only those with adequate level background investigations are granted access to sensitive/private information. HUD ensures this through the HUD Acquisition Regulations (HUDAR) general clause governing access to systems, as well as contract-specific clauses. These various contract clauses enforceprocedures that contractors must follow to ensure that all contractors have had the background investigation appropriate for their level of access to sensitive systems or data. Additionally, standard operatiing 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?

The enrollment record can only be viewed or retrieved by a PIV Registrar 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 (and have been certified and accredited) can retrieve or view enrollment information. HUD's certifying agent for PIV will evaluate the technical and operational controls at each location where PIV Registrar functions are performed, and recommend to the designated accreditation authority (Assistant Secretary for Administration) the improvements that are needed at each location (Headquarters and about 50 HUD Field Offices).

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

For example, if a decision was made to increase the number of user roles so that access to information was further tightened, include such a discussion.

SECTION 7.0 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 in accordance with *the National Archives and Records Administration (NARA) General Records Schedule for records pertaining to this program relevant to both the PIV I and PIV II*.

For employees and contractors currently working at HUD, data in the IDMS and CMS will be kept in the active databases for the duration of their employment with HUD. When the employee or contractor leaves HUD, data will be archived off-line for 7 years, then deleted.

SECTION 8.0 RESULTS OF FISMA REVIEW

8.1 Have the system(s) completed a C&A as required by the Federal Information Systems Management Act (FISMA)?
Not yet. The C&A of HUD Headquarters IDMS and CMS is expected by June 2007.

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

8.3 Has the agency conducted a risk assessment, and identified and implemented appropriate technical, administrative, and operational security controls? [*List each type of control.*]

SECTION 9.0 ANALYSIS AND ASSESSMENT

[*Describe your agency's analysis and assessment.*]

This PIA cannot be considered final until the formal C&A of the IDMS and CMS is completed – which is expected by June 2007. When the C&A is available, then Sections 8-10 of this PIA can be updated.

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(s).

9.2 Did you evaluate competing technologies to assess and compare their ability to effectively achieve the program's goals?

9.3 If applicable, describe the competing technologies.

9.4 Describe the changes made to the PIV program due to the assessment:

9.5 What unique issues does this program present?

9.6 What specific strategies are used to address these issues?

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

SECTION 10.0 CONCLUSIONS

[*Summarize the privacy risks identified in the above questions and the means by which you have mitigated and/or considered those risks.*]

This PIA cannot be considered final until the formal C&A of the IDMS and CMS is completed – which is expected by June 2007. When the C&A is available, then Sections 8-10 of this PIA can be updated.
In the meantime, the following "ACTIONS NEEDED" were identified in the PIA sections above, as noted:

- **Sec. 6.1:** Consequences for violating privacy policies are outlined generally in HUD's Privacy Act Handbook.
- **Sec. 6.1:** "Continuous auditing of compliance with stated privacy policies and practices…" will be conducted.
- **Sec. 6.1:** A system security plan as well as a certification and accreditation (C&A) of the identity management system (IDMS) and card management system (CMS) will be prepared. These are in process (due by June 2007), led by the Office of the Chief Information Officer, with support from the Office of Security and Emergency Planning (OSEP).
- **Sec. 6.2:** A system security plan as well as a certification and accreditation (C&A) of the identity management system (IDMS) and card management system (CMS) will be prepared. These are in process (due by June 2007), led by the Office of the Chief Information Officer, with support from the Office of Security and Emergency Planning (OSEP). These documents will cover the 8 areas below, as required by NIST Special Publication 800-53.
- **Sec. 6.5: ACTION NEEDED:** HUD's certifying agent for PIV will evaluate the technical and operational controls at each location where PIV Registrar functions are performed, and recommend to the designated accreditation authority (Assistant Secretary for Administration) the improvements that are needed at each location (Headquarters and about 50 HUD Field Offices).

SECTION 11.0 DETERMINATIONS OF OFFICIALS

The sensitivity of this system requires HUD to ensure that it meets the following requirements:

- Achieve an IT Security certification and accreditation (C&A)every three years (following NIST Special Publication 800-37).
- Review associated Privacy Act System of Record Notices (SORNs) every other year, and re-publish in the Federal Register if revisions are needed.
- Review and update as necessary applicable Privacy Impact Assessments (PIAs) (following OMB Memorandum M-03-22).

Contingent on the three elements listed above, comments in Sec. 10, and fulfilling all applicable Directives, OMB guidance, and NIST standards and requirements, the privacy controls related to the system this PIA covers are considered adequate.