Office of Human Resources

PERSONAL IDENTITY VERIFICATION – PRIVACY IMPACT ASSESSMENT

INTRODUCTION

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. This policy is intended to enhance security, increase efficiency, reduce identity fraud, and protect personal privacy.

HSPD-12 requires that Federal credentials 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 20l (FIPS 201), Personal Identity Verification (PIV) of Federal Employees and Contractors.

FIPS 201 has two parts: PIV I and PIV II. The requirements for 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 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. FIPS 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, the Office of Human Resources is responsible for the identity management and all aspects of the National Credit Union Administration (NCUA) 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. NCUA is currently expecting to issue approximately 960 PIV cards beginning in 2007.

PRIVACY IMPACT ASSESSMENT SCOPE

This Privacy Impact Assessment (PIA) provides details about the National Credit Union Administration's role in the collection and management of personally identifiable information for the purposes of issuing credentials (ID cards) to meet the requirements of HSPD-12 and comply with the standards outlined in FIPS 201 and its accompanying special publications. 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: (1) background investigation; (2) identity proofing and registration; (3) Identity Management System (IDMS), the database used for identity management; and (4) the PIV card.

As stated previously, PIV-I requires the implementation of registration, identify proofing, and issuance procedures compliant with the standards of FIPS 201. However, the collection of information for background investigations has been a long-standing requirement for Federal employment. This process and the elements used are not new. The forms and information collected for the background investigation process will continue to occur. The implementation of PIV may require a new system or new technology. However, NCUA will continue to issue existing ID cards under PIV-I, but the process for credential application and issuance will conform to the 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 the National Credit Union Administration PIV Program and the credential issued referred to as PIV cards.

BASIC CONTROL ELEMENTS

There are four control objectives of the PIV program: 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 identify 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.

The Agency's PIV implementation must meet the four control objects such that:

- PIV Cards are only issued (1) to individuals whose true identity has been verified, and (2) after a proper authority has authorized issuance of the credential.
- Only an individual with a completed background investigation on record is issued a PIV Card.
- An individual is issued a PIV Card only after presenting two-identity source documents, at least one of which is a valid Federal or state government 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 PIV Card.
- No substitution occurs in the identity-proofing process. Specifically, the individual who appears for identity proofing and whose fingerprints are checked, is the person to whom the PIV Card is issued.
- No PIV Card is issued unless requested by a proper sponsor.
- A PIV Card remains serviceable only up to its expiration date. A revocation process exists such that expired or invalidated credentials are swiftly revoked.
- An issued PIV Card is not modified, duplicated or forged.

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, a Federal employee or a contractor. As required by FIPS 201, NCUA will collect biographic and biometric information from the PIV Applicants in order to: (1) conduct the background investigation; (2) complete the identity-proofing and registration process; (3) create a data record in the PIV Identity Management System (IDMS); and (4) issue a PIV card. Table I shows what information is collected from the PIV Applicant in relation to each of these processes.

Table 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				
Social Security Number (SSN)	X	X	X		
Other Names Used	X				
Citizenship	X				
Other identifying information (height, weight, hair color, eye color, gender)			Optional	Optional	
Organizational affiliation (e.g., Contractor, Active Duty, Civilian)	X	X	X	X	X
Employee Affiliation (e.g., Contractor)		X	X	X	X
Fingerprints (10)	X	X	X		

Biometric identifiers (2 fingerprints)		X	X		X
Digital color photograph		X	X	X	X
Digital signature			X	X	X
Telephone numbers	X		X		
Spouse (current or former), relatives and associates, information regarding their citizenship	X				
Marital status	X				
Employment history	X				
Address history	X		X		
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		
Signed SF-85 or equivalent	X		X		
Copies of identity source documents	X		X		

1.2 What is the information used for?

The information identified in Table 1 is used in each step of the PIV processes as described below:

1. Conduct a background investigation. The PIV background investigation as required by FIPS 201 is a condition of Federal employment which includes contractors and matches PIV Applicant 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 Public Trust Positions, Standard Form 85P (SF-85P) or the Questionnaire for National Security Positions, Standard Form 86 (SF-86). Standard Form process entails conducting a full National Agency Check (NAC) or National Agency Check with Inquiries (NACI), which are described below:

- NAC: Consists of searches of the OPM Security/Suitability Investigations Index (SII), the Defense Clearance and Investigations Index (DCII), the Federal Bureau of Investigation (FBI) Identification Divisions' name and fingerprint files, and other files or indices when necessary.

- NACI: The basic and minimum investigation required on all new Federal employees consisting of a NAC with written inquiries and searches of records covering specific areas of an individual's background during the past five years.

2. Complete the identity proofing and registration process. Biometrics are used to ensure PIV Applicants have not been previously enrolled in the NCUA 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. 15-0316, Employment Eligibility Verification.

3. Create a data record in the PIV Identity Management System (IDMS). The IDMS is used during the registration process to create the PIV Applicant's pre-enrollment and enrollment record, manage and maintain this information throughout the PIV card lifecycle, and verify, authenticate and revoke PIV cardholder use.

4. 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. Once the individual has been issued a PIV card, the IDMS is updated to reflect that the card has been issued.

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

Additionally, the NCUA PIV IDMS and PIV cards contain other data not collected from the PIV Applicant that are either (1) electronically stored on the card; (2) electronically stored in the IDMS; and/or (3) physically displayed on the card. This information and the purpose of its use is described in Table 2.

Table 2: Other PIV Information Stored, Collected or Used

	IDMS (Electronically Stored)	PIV Card (Physically Displayed)	PIV Card (Electronically Stored)	Purpose
Card Expiration Date	X	X	X	To verify card is valid and allow access to facilities and computer systems
Agency card serial number	X	X		For identifying and maintaining
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.

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 the NCUA employees and contractors involved in the design, development, implementation, and execution of the NCUA 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 NCUA employees and its contractors who have a "need to know" for implementation of the National Credit Union Administration PIV Program. NCUA contractors are contractually obligated to comply with the Privacy Act in the handling, use and dissemination of all personal information.

NCUA uses the role-based model for PIV and the critical roles are described below. All individuals will be trained to perform his or her respective role; however, these roles may be additional roles assigned to personnel who have other 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 Card to the Applicant. PIV Sponsors shall meet the following minimum standards: (1) is a Federal Government employee and be authorized in writing by the Office of Human Resources to request a PIV credential; (2) have valid justification for requesting a PIV Card for an Applicant; and (3)have already been issued a valid PIV Card.

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

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

2. **PIV Registrar.** The individual 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 Card to the Applicant. PIV Registrars shall meet the following minimum standards: (1) is a Federal Government official and is designated in writing as a PIV Registrar; (2) 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 (3) is capable of evaluating whether a PIV application is satisfactory.

   The PIV Registrar has access to the following information:
   - Applicant's SF-85P, or SF-86
   - Two forms of identity source documents

   The PIV Registrar will record the following data for each of the two identity source documents, sign the records and keep it on file:
   - Document title
   - 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 info) with the corresponding information provided by the applicant at an earlier visit.
- Reviews the captured facial image of applicant and retains a copy of the image.
- Ensures fingerprints of the applicant have been taken and retains a copy.
- Initiates at a minimum, a NACI.
- Notifies the Sponsor and designated PIV Issuer the applicant has been approved for hire or not.

3. **PIV Issuer.** This individual performs credential personalization operations and issues the PIV Card to the Applicant after all background checks, identity proofing, and related approvals have been completed.

   The PIV Registrar makes available the following information to the PIV Issuer:
   - Facial image copy
   - Result of background investigation
   - Other data associated with applicant (e.g., employee affiliation)

4. **PIV Adjudicator.** The individual responsible for determining whether the Applicant is suitable to receive a PIV Card, based on results obtained from the OPM background investigation. Adjudicator responsibilities include: (1) confirming fingerprint results from OPM/FBI; (2) adjudicating NACI (or higher-level OPM investigation) and resolving issues if necessary; (3) providing final results to the PIV Registrar; and (4) updating the Official Personnel Folder (OPF) with "Certificate of Investigation."

SECTION 3.0 EXTERNAL SHARING AND DISCLOSURE

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

During the initial background investigation process and identity proofing, relevant personal data will be:

1. Shared with the OPM who is responsible for conducting the NACI and other higher-level investigations for NCUA; and
2. Matched against databases at the Federal Bureau of Investigation (FBI) to prevent the hiring of applicants with a criminal record or possible ties to terrorism.

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

- An appropriate government law enforcement entity if records show a violation or potential violation of the law;
- The Department of Justice, a court, or other adjudicate 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 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.

SECTION 4.0 PRIVACY ACT REQUIREMENTS

4.0 As required by the Privacy Act, 5 USC 552(a)(e)(3), Privacy Act information is provided to the individual at the time information is collected. The notice states the reasons for collecting information, the consequences of failing to provide the requested information, and explains how the information is used. The collection, maintenance, and disclosure of information complies with the Privacy Act and the published System of Records Notice for the Background Investigation Files and the Personal Identity Verification Files.

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

Applicants must provide the information requested for the PIV Program. Failure to provide any of the requested information will provide NCUA with grounds for not offering them employment for more than 6 months and limited access to the NCUA premises and any other Federal facility. However, access to NCUA premises or other facilities may be a necessary prerequisite to the Applicant retaining employment longer than 6 months or performing a contract. Any false information that is provided in response to a question required under the PIV Program may be grounds for denying employment, dismissal after work is commenced, or refusing access to NCUA's or other Federal facility and may be punishable by fine or imprisonment.

4.2 What are the procedures for ensuring that the information maintained is accurate, complete, and up-to-date?

The process for issuing a PIV Card requires independent verification of identity source documents by both the regional office and central office ensuring that the data maintained is accurate and complete. PIV credentials are valid for a period not to exceed 5 years. Before an expired card can be reissued, OHR will validate all necessary identity documents are on file and current. OHR will also verify the cardholder's identity against the electronic facial image and fingerprints stored on the expiring card.

4.3 What is the length of time the information will be retained, and how will it be purged?

Information will be destroyed five years after separation or transfer of an employee, or five years after the contract relationship expires, whichever is applicable. If NCUA receives notification of

the individual's death prior to that time, the information will be destroyed promptly upon notification. Paper documents are destroyed by shredding. Electronic information is destroyed by deleting information from the appropriate database(s).

4.4 What administrative and technological procedures are used to secure the information against unauthorized access?

Paper copies of the information are maintained in a secure manner in locked rooms in locked file cabinets. Information maintained on computers will be secured using both administrative and technological controls. The PIV process incorporates security safeguards and are compliant with the agency's information technology security protocol as well as password and remote access policies. Periodic testing of the process controls will be conducted annually as part of the ongoing maintenance of the PIV certiication and accreditation process.

A security assessment based on the guidelines in FIPS-201 will be completed annually in order to ensure adherence to guidance outlined in FIPS-201 and its supporting publications. The potential risk of inappropriate disclosure and/or unauthorized disclosure will be mitigated by limiting the number of authorized users.

4.5 Is a system of records being created under the Privacy Act, 5 U.S. C. 552a?

The system of records *Personal Identity Verification Files* applies to the PIV process and related records.