



**Homeland Security Presidential Directive 12 (HSPD-12)
Personal Identity Verification, Part-1 (PIV-1)**

Privacy Impact Assessment

May 2006
Credential Management Program Office
Office of Security

SCOPE AND BACKGROUND

This is the first of a series of Privacy Impact Assessments (PIA) that the Department of Commerce will develop to describe the privacy protections for the personal information that is collected and maintained in the process of issuing enhanced and more secure identification (ID) cards and ensuring the security of Commerce facilities.

This initial PIA describes the process that Commerce has developed to comply with the requirement that all federal agencies develop and implement a new standardized process for verifying the identity of employees and contractors prior to issuance of an ID card or badge. This requirement is based on Homeland Security Presidential Directive 12 (HSPD-12), Policy for a Common Identification Standard for Federal Employees and Contractors (August 27, 2004).

Based upon this directive, the National Institute for Standards and Technology (NIST) developed Federal Information Processing Standards Publication (FIPS Pub) 201, Personal Identity Verification (PIV) of Federal Employees and Contractors (February 25, 2005)

FIPS-201 provides specific guidance to agencies about how to implement HSPD-12. It specifies the architecture and technical requirements for a common identification standard for Federal employees and contractors. The overall goal is to achieve appropriate security assurance for multiple applications by efficiently verifying the claimed identity of individuals seeking physical access to Federally controlled government facilities and electronic access to government information systems.

There are two major sections in FIPS-201. Part One ("PIV-1") describes the minimum requirements for a Federal personal identity verification system that meets the control and security objectives of HSPD-12, including personal identity proofing, registration, and issuance.

PIV-1 is intended to ensure the integrity of the process for verifying the identity of employees and contractors who are issued an ID card. This PIA describes the PIV-1 process in Commerce, which started implementing the HSPD-12 program on October 11, 2005. It also describes the process for the actual issuance of ID cards throughout Commerce pending implementation of PIV-2, below.

FIPS-201, Part Two ("PIV-2") provides the technical specifications for the new ID "smart" card and federal agency PIV systems so that they are interoperable. The PIV-2 requirement is being developed in Commerce, and will be implemented by October 2007. PIV-2 is not covered in this PIA, but will be addressed in subsequent PIAs after implementation.

The implementation of HSPD-12 will result in major changes in the issuance of Federal ID cards and badges. A supervisor will no longer have the authority to initiate and approve an ID card. Only designated Sponsors, who have completed the required training, will be authorized to initiate the ID card process. In Commerce, Sponsors will be selected from Human Resources (HR) personnel and Contracting Officer Representatives (CORs).

The new Personal Identity Verification (PIV) process includes the following requirements:

- An employee or contractor who applies for an ID card must receive a favorable background investigation report prior to issuance. For most individuals this involves a Federal Bureau of Investigation (FBI) fingerprint check, and a National Agency Check with Inquiries (NACI), i.e., a search of law enforcement and arrest records and a credit check. For individuals in positions that require a security clearance, a more detailed background investigation will be conducted.
- Each applicant must present two forms of identification.
- The same official may not be responsible for requesting, authorizing, and issuing an ID card.

There are also new terms and responsibilities associated with this process:

- Personal Identity Verification (PIV) card is the new term for ID cards.
- Applicants are employees and contractors who apply for a PIV card.
- Registrars, mainly located in the Commerce Regional Security Offices, are responsible for authorizing the issuance of the cards.
- Enrollment Officials and Remote Issuers have other additional roles.
- PIV Card Issuing Facilities (PCIFs) are the approximately ten Commerce facilities throughout the continental United States that are authorized to issue PIV cards.
- The CD-591, PIV Request, is the only form authorized for use in Commerce to request, process, and acknowledge receipt of a PIV card.

What information is to be collected (e.g., nature and source)?

PIV Card Sponsors use the CD-591 collect and record personal information about the applicant from other records and information systems, and is used to track the issuance of the PIV card from application to issuance, receipt, and acknowledgement. It also serves to transmit source documents that are necessary to process the application, e.g., fingerprint card and Form I-9, Employment Eligibility Verification.

The elements of the CD-591 indicate the information that is collected and the source:

- Section A, PIV Request and Source Document Confirmation, consists of the name, organization, and contact information about the applicant, and is completed by the sponsor.
- Section B, Identity-Proofing, is completed by the sponsor, registrar, or enrollment official. It verifies that the applicant presented two forms of identification and appeared in person before the signing official.
- Section C, Card Approval, is used by the registrar to certify that the appropriate investigation has been completed with a favorable result, and that issuance of the card is approved.
- Section D, Card Details, indicates the name on the card, card number, and expiration date, and is signed by the issuing facility representative.
- Section E, Applicant Acknowledgement, is signed by the applicant upon receipt of the card.

Prior to the request for a PIV card, the applicant will have completed one or more forms that are used to collect personal background information. These forms all have approved information collection numbers from the Office of Management and Budget (OMB), and the OMB approval number and the date of expiration are at the top right hand corner of each form.

The forms are:

- Form I-9, Employment Eligibility Verification;
- Standard Form (SF) 85, Questionnaire for Non-Sensitive Positions;
- SF 85P, Questionnaire for Public Trust Positions; and
- SF 86, Questionnaire for National Security Positions.

The completed form(s) were submitted to Human Resources and/or the Office of Security as part of entry on to duty processing, application for a security clearance, or some other event, and they will accompany the PIV Request

The table below itemizes many of the data elements that are or may be collected on the above form(s) or as part of the entry on duty processing. Except for the signature in digital form and the two additional biometric fingerprints, all the information collected from the employee or contractor is unchanged since the forms were approved by OMB.

Fingerprints (10)
Biometric identifiers (2 fingerprints)
Digital signature
Telephone numbers
Spouse (current or former), relatives and associates, information regarding their

citizenship
Marital status
Employment history
Address history
Educational history
Personal references
Medical Record
Military history/record
Illegal drug history
Criminal history
Use of alcohol
Foreign activities
Foreign countries visited
Background investigations history
Financial history
Association history

This information is maintained in the PIV Identity Data Management System (IDMS).

Why is the information being collected?

The PIV-1 process does not involve the collection of personal information from individuals that was not collected previously with approval from OMB, in accordance with the provisions of the Paperwork Reduction Act. Instead, it establishes a more secure and reliable process for the verification of the identity of the individual employee or contractor and the subsequent issuance of the PIV card to that individual.

The PIV-1 process and the related use and maintenance of personal information about applicants is required under HSPD-12, and is being collected and maintained in accordance with the guidance in FIPS-201.

Although the information collected is not new, HSPD-12 requires that this information must be provided by all prospective and current federal employees and contractors. Consequently, the scope and size of the universe from which the information is collected has greatly expanded. Previously, only applicants for a security clearance and employees in sensitive positions were subject to a full-field background investigation and had to provide the personal information described above in support of the investigation. The background investigations for other employees and contractors were generally limited to a NACI.

PIV Card Applicants may address privacy-related matters to the DOC Agency Official for Privacy. PIV Card Applicants who are denied a PIV card because of missing or incorrect information may request assistance from the DOC

Card Applicant Representative in the Credential Management Program Office. In the event that the PIV Card application is denied due to a disqualifying factor, the Applicant has the option to begin the [appeals process](#) outlined on the Department of Commerce Office of Security HSPD-12 Web page.

What is the intended use of the information?

The information is intended to ensure that ID cards issued by the federal government to its employees and contractors are secure and accurate and can be relied upon by federal agencies, citizens, and others.

Secure, accurate, and reliable forms of identification are those that are:

- Based on sound criteria for verifying an individual employee's identity;
- Very resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation;
- Capable of rapid electronic authentication; and
- Issued by officially accredited providers.

With whom will the information be shared?

The PIV card contains limited information about the individual: frontal face photograph, full name, agency, organization, card expiration date, agency card serial number, and issuer identification number. The card also stores a Personal Identification Number (PIN), cardholder unique identifier, authentication key, and two electronic fingerprints.

DoC and other agencies will use the card when the individual requires and requests access to federal facilities, computer systems, applications or data, in order to verify the individual's identity and right of access.

What opportunities do individuals have to declines to provide information or to consent to particular uses of the information?

The PIV-1 process does not involve the collection of new information from the individual but uses information that was previously provided as part of the individual's entry on to duty processing, application for a security clearance, or some other event.

How will the information be secured (e.g., administrative and technological controls)?

The information will be secured using both administrative and technological controls. The PIV-1 process will incorporate security safeguards and will be compliant with the Department's Information Technology Security Program (ITSP) Policy and Minimum Implementation Standards as well as the Department's Password and Remote Access Policies.

Periodic testing of the process controls will be conducted at least annually as part of the ongoing maintenance of the PIV-1 process certification and accreditation.

A security assessment for this process has been completed in order to ensure adherence to guidance outlined the 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.

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

The system of records [COMMERCE/DEPT-13](#), "Investigative and Security Records," applies to the PIV-1 process and related records.