

**Small Business Administration**  
**Privacy Impact Assessment**

**Name of Project: Personal Identity Verification (PIV)/ Homeland Security  
Presidential Directive 12 (HSPD-12)**

(Note: This PIA is intended to cover the overall operational aspects of the PIV-I process in the Agency and it is not a program level PIA that would cover the processes and procedures for PIV-I.) Other more detailed Privacy Impact Assessments are developed to address the handling of information for: (1) Security background checks; (2) the physical access PIV card; (3) logical access; and (4) organizational information and electronic certification information identified in the access directory.

Once the PIA is completed and the signature approval page is signed, please provide copies of the PIA to the following:

- SBA IT Security Manager
- SBA OCIO IT Portfolio Division
- SBA Privacy Officer

**Do not email the approved PIA directly to the Office of Management and Budget email address identified on the Exhibit 300 form. One transmission will be sent by the OCIO Portfolio Management Division.**

**Also refer to the signature approval page at the end of this document.**

**A. CONTACT INFORMATION**

**1) Who is the person completing this document?**

Kenneth T. Etheridge  
Director  
Office of Administration  
(202) 205-7028  
[Kenneth.etheridge@sba.gov](mailto:Kenneth.etheridge@sba.gov)

Ravoyne Payton  
Information Technology Specialist  
Office of the Chief Information Officer  
(202) 205-7168  
[Ravoyne.payton@sba.gov](mailto:Ravoyne.payton@sba.gov)

**2) Who is the system owner?**

Robert Danbeck  
Associate Administrator  
Office of Management & Administration  
(202) 205-6610  
[Robert.danbeck@sba.gov](mailto:Robert.danbeck@sba.gov)

Christine Liu  
Chief Information Officer & Chief Privacy Officer  
(202) 205-6708  
Christine.liu@sba.gov

**3) Who is the system manager for this system or application?**

Security background checks  
Linda Roberts  
Office of Inspector General  
(202) 205-6223  
Linda.roberts@sba.gov

Physical access PIV card  
Kenneth T. Etheridge  
Director  
Office of Administration  
(202) 205-7028  
Kenneth.etheridge@sba.gov

PIV Card Logical access  
Ravoyne Payton  
Information Technology Specialist  
Office of the Chief Information Officer  
(202) 205-7168  
Ravoyne.payton@sba.gov

**4) Who is the IT Security Manager who reviewed this document?**

David L. McCauley  
Chief Information Security Officer  
Office of the Chief Information Office  
(202) 205-7103  
david.mccauley@sba.gov

**5) Who is the Bureau/Office Privacy Act Officer who reviewed this document?**

Ethel Matthews  
Senior Advisor to the Chief Privacy Officer  
(202) 205-7173  
Ethel.matthews@sba.gov

**6) Who is the Reviewing Official?** (According to OMB, this is the agency CIO or other agency head designee, who is other than the official procuring the system or the official who conducts the PIA).

Christine H. Liu  
Chief Information Officer & Chief Privacy Officer  
(202) 205-6708  
Christine.liu@sba.gov

## **B. PIV PROCESS APPLICATION/GENERAL INFORMATION**

### **1) Does this system contain any information about individuals?**

#### **a. Is this information identifiable to the individual<sup>1</sup>?**

Yes

#### **b. Is the information about individual members of the public?**

No.

#### **c. Is the information about employees?**

Yes

### **2) What is the purpose of the PIV Process?**

Homeland Security Presidential Directive 12 (HSPD-12) directs the use of a common identification credential for both logical and physical access to federally controlled facilities and information systems. This policy is intended to enhance security, increase efficiency, reduce identity fraud, and protect personal privacy.

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

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

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

---

<sup>1</sup> "Identifiable Form" - According to the OMB Memo M-03-22, this means information in an IT system or online collection: (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors).



The PIV consists of the process required for personal identity verification including the standard background investigation required for all Federal employees and long-term contractors. It also includes the issuance of a smart card. These processes result in several collections of information and more detailed Privacy Impact Assessments are developed for each of these repositories of information: for (1) Security background checks; (2) the physical access PIV card; (3) logical access; and (4) organizational information and electronic certification information identified in the access directory

### **3) What legal authority authorizes the purchase or development of this PIV Process?**

Homeland Security Presidential Directive 12 (HSPD-12), issued by President George W. Bush on August 27, 2004, mandates 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.

The following are authorities to cover each step of the Personal Identity Verification process:

- Civil Service Act of 1883, Section 2
- Public Law 82-298
- Public Law 92-261
- Public law 93-579
- Public Law 107-347
- 5 U.S.C. (Title 5, U.S. Code), sections 552a, 1303, 1304, 3301, 7701
- 22 U.S.C., sections 1435, 2519, 2585
- 32 U.S.C., section 686
- 40 U.S.C., section 11302 (e)
- 42 U.S.C., sections 1874 (c), 2165, 2455
- 5 CFR (Title 5, Code of Federal Regulations), part 5
- Federal Information Processing Standards 140-2, 199, 201
- National Institute of Standards and Technology (NIST) Special Publications 800-37, 800-53, 800-63, 800-73, 800-76, 800-78, 800-79, and 800-85.

## **C. DATA IN THE PROCESS**

### **1) What categories of individuals are covered in the PIV Process?**

Information will be maintained on individuals for the PIV-I process who are identified in Office of Management and Budget HSPD-12 guidelines and FIPS 201. The process will cover individuals such as:

- Employees who work in the SBA facilities defined in title 5 (5 U.S.C.) Sec. 2105;
- Contractors requiring access to SBA facilities and systems;
- Volunteers and temporary employees;

- Other persons who are visiting SBA facilities who have been issued PIV cards from other agencies; and
- It does not apply to occasional visitors or short-term guests

**2) What are the sources of the information in the PIV Process?**

**a. Is the source of the information from the individual or is it taken from another source? If not directly from the individual, then what other source?**

Information in the system is derived mostly from the individual. Other information from other sources comes from other different points in the PIV card registering, issuing, and management systems, and in use of the PIV card.

Most information taken from the individual comes from (1) Background investigation files; Identity proofing and registration (enrollment) of employees and contractors; the identity management system and associated systems/databases which track/control all information needed for the new Personal Identity Verification process; and personal information contained on the new PIV card.

**b. What Federal agencies are providing data for use in the process?**

Department of Justice (DOJ), Civil Applicant System (CAS), and Integrated Automated Fingerprint Identification System (IAFIS) provides the wrap sheet results back to the Inspector General.

**c. What Tribal, State and local agencies are providing data for use in the process?**

None

**d. From what other third party sources will data be collected?**

Credit Check Agencies

**e. What information will be collected from the employee and the public?**

As required by FIPS 201, and the PIV card registration and issuance procedures, and required in Form I-9, OMB No. 115-0316, Employment Eligibility Verification. SBA will collect/maintain the following information on the applicant/user: Name (Last, First, and middle initial)

- Date of birth
- Social Security Number (SSN)
- Place of birth
- Organizational affiliation
- Employee affiliation (e.g., Contractor, Active Duty, Civilian)
- Biometric identifiers (e.g., fingerprint, voiceprint)
- Electronic signature
- Digital photograph
- Personal Identification Number

- PIV authentication key
- Cardholder unique identifier
- Signed PIV requests
- Signed SF 85 (or equivalent)
- Results of background check
- PIV Registrar approval (digital signature)
- Card expiration date
- Agency card serial number
- Copies of identity source documents
- ID source document title
- ID source document issuing authority
- ID source document number
- ID source document expiration date
- ID source document other information

### 3) Accuracy, Timeliness, and Reliability

**a. How will data collected from sources other than SBA records be verified for accuracy?**

The HSPD-12 system does not collect data from sources beyond the identification presented by the prospective employee or contractor. Standard information collected is:

- Name
- Social Security number
- Address
- Citizenship
- Document expiration date
- Passport and Driver's License are scanned into the HSPD-12 system

**b. How will data be checked for completeness?**

The HSPD-12 enroller asks the presenter of the information to review the information captured for accuracy and completeness.

**c. Is the data current?** What steps or procedures are taken to ensure the data is current and not out-of-date? Name the document (e.g., data models).

HSPD-12 enroller and the individual presenting the documentation are responsible for ensuring that the identification documentation presented is current.

**d. Are the data elements described in detail and documented?** If yes, what is the name of the document?

The data elements captured by HSPD-12 are described in the agency PCI Operations document.



## D. ATTRIBUTES OF THE DATA

- 1) **Is the use of the data both relevant and necessary to the purpose for which the process is being designed?**

Yes. The Agency examined what information was required according to FIPS 201. SBA considered the collection and maintenance of only information absolutely necessary for the individual to obtain a PIV card. The PIV card process itself will help to eliminate maintenance of redundant systems and processes and therefore increasing privacy protection of the individuals involved in the card issuance.

- 2) **Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected, and how will this be maintained and filed?**

Yes. The HSPD12 initiative collects certain information not normally obtained in the past of some employees (i.e. biometric information), and contractors (i.e., background checks). New information collected was a result of being compliant with FIPS 201 requirements. As a means of encouraging privacy protection most systems created as a result of the process are maintained separately and by different system managers. However, aggregation of certain information from these systems will be required in order to complete the issuing process and collected as a result of use of PIV cards for system and physical access.

- 3) **Will the new data be placed in the individual's record?**

The employee Unique Private Name, biometric data, and photo of the individual will be maintained in the system. All of these items were previously collected in paper format and separate systems.

- 4) **Can the system make determinations about employees/public that would not be possible without the new data?**

No, all the data collected with the exception of the biometric data has all been previously collected or inspected during the hiring process.

- 5) **How will the new data be verified for relevance and accuracy?**

FIP201 addresses this issue. In addition, each role holder in the system (sponsor, enroller, adjudicator, and issuer) has the ability to verify data, and return to the previous role holder if questions arise.

- 6) **If the data is being consolidated, what controls are in place to protect the data from unauthorized access or use?**

The system can only be accessed with a PIV II card, personal identification pin, and the issuance of system rights.

- 7) **If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access through the process? Explain.**

Each collection of information and system identified in the PIV process will have a separate Certification and Accreditation performed which will include separate Privacy Impact Assessments.

These systems are all covered by separate Privacy Act system of records notices and have separate business rules identified to ensure that employees comply with the requirements of the Privacy Act and Department of the Interior privacy Act regulations at 43 CFR 2.51. System Managers for each system are responsible for the administration of appropriate safeguards to protect the information collected, maintained and transmitted.

- 8) **How will the data be retrieved? Does a personal identifier retrieve the data? If yes, explain and list the identifiers that will be used to retrieve information on the individual.**

**Data can be searched and retrieved in the system by:**

- Office/Organization
- Employee first or last name
- Affiliation (Contractor)
- Last 4 of social security number
- Workflow status

- 9) **What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?**

Reports are not produced on individuals. Status reports on the number of individuals in queue, and at which stage they are in the process. System Organization Administrators have access to this report.

- 10) **What opportunities do individuals have to decline to provide information (i.e., where providing information is voluntary), or to consent to particular uses of the information (other than required or authorized uses), and how individuals can grant consent.)**

The background investigation (full NACI) is a condition of Federal employment (now extended to contractors). 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).



## **E. MAINTENANCE AND ADMINISTRATIVE CONTROLS**

- 1) If the information in the process operated in more than one site, how will consistent use of the data be maintained in all sites?**

More detailed Privacy Impact Assessments are developed to address the handling of information for: (1) Security background checks; (2) the physical access PIV card; (3) logical access; and (4) organizational information and electronic certification information identified in the access directory. Separate IT Security Certifications with Security Plans and Business Rules will be performed to ensure that use is consistent with the separate Privacy Act system of records notice and intention of the collection of the information identified on the forms collecting the information.

For paper record processes, system managers for these collections are responsible for ensuring that appropriate security procedures are in place to protect the information and ensure that the information is used as described in the different Privacy Act notices.

- 2) What are the retention periods of data in this system?**

**SBA 34 – Identity Management System defines the retention period.**

- (1) Security background checks: Five years
- (2) The physical access PIV card: Duration of employment with SBA.
- (3) Logical access: Duration of employment with SBA or authorized access.
- (4) Organizational information and electronic certification information identified in the access directory: Duration of employment with SBA or SBA organization.

- 3) What are the procedures for disposition of the data at the end of the retention period? How long will the reports produced be kept? Where are the procedures documented?**

The HSPD-12 system utilizes the SBA standard disposition of data process.

- (1) Security background checks: The Office of Inspector General's SOPs are followed.
- (2) The physical access PIV card: Upon termination of employment with SBA, the PIV card is collected with other agency issued equipment.
- (3) Logical access: Upon termination of employment, logical access is terminated via either the help desk or the organizational IT Security Specialist.
- (4) Organizational information and electronic certification information identified in the access directory: Electronic certificates are revoked when the PIV card is canceled by the issuer.

- 4) Are the systems in the process using technologies in ways that the SBA has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)?**

Yes. This technology modifies the manner in which information is collected of employees and government contractors. The information collected in order to issue a PIV credential is the same as the processes previously used. This technology allows the agency to capture a digital image of the I9 paperwork previously submitted in accordance with the Illegal Immigration Reform and Immigrant Responsibilities Act

(IIRIRA) of 1996. In addition to the digital image of the I9 documentation, this system also captures biometric data of the individual.

Privacy is affected via the collection of biographical, bio-metric, background investigation data, other data used by the agency to determine suitability for employment.

**5) How does the use of this technology affect public/employee privacy?**

This technology automates the collection of identification I9 documentation previously provided only in paper. The process of collecting identification information for employment purposes is a long standing agency practice required by the IIR&IRA of 1996.

Role holders must complete the PIV process and be issued a PIV credential in order to access the system. The four functions required in the PIV process can access the system and individual records. Role holders are (1) Sponsor, (2) Enroller, (3) Adjudicator, and (4) Issuer.

Role holder must have in their possession their assigned PIV credential, and enter their personal identification number in order to access the system. Once logged in the system will only allow the role holder to access views in which they hold a role. In addition to the credential and the personal identification number, the system will verify the public key infrastructure certificate on the PIV credential to ensure that the card has not been revoked.

**6) Will this system in this process provide the capability to identify, locate, and monitor individuals? If yes, explain.**

If the PIV II card is used to log on and off the network as well as access physical work space, then data on past activities will be available for collection. For example, using the PIV II card to exit a building in the event of an emergency will provide the agency with a real time roster of employees, there by allowing search and rescue personnel to restrict search activities to those who have not checked in and to their last logged location.

This system does not currently offer the ability to provide real time identity, location, and monitoring capabilities.

**7) What kinds of information are collected as a function of the monitoring of individuals?**

There is no information collected as a function of monitoring of individuals. Information collected is a subset of information required by the Questionnaire for Public Trust Positions (85P), and the Eligibility Employment Verification (I9).

**8) What controls will be used to prevent unauthorized monitoring?**

There is currently no monitoring of individuals.



**9) Under which Privacy Act systems of records notice does the system operate? Provide number and name.**

- (1) Identity Management System – SBA 34
- (2) Security background checks: Personnel Security Files – OS-45
- (3) The physical access PIV card: Computerized ID Security System – OS-1
- (4) Organizational information and electronic certification information identified in the access directory: Enterprise Access Control System – SBA-30

**10) If the system is being modified, will the Privacy Act system of records notice require amendment or revision? Explain.**

If the system is modified to collect or retain additional privacy information beyond what has already been identified, then the system of record notice may require revision.

**F. ACCESS TO DATA**

**1) Who will have access to the data in the system? (e.g., contractors, users, managers, system administrators, developers, tribes, other)**

FIPS 201 defined role holders and SBA defined organizational administrators will have access to data specific to their role. An individual must be granted rights by another PIV role holder, have a valid PIV card in order to access the system and its data.

System developer contractors with designated rights, and a PIV card have access the system.

**2) How is access to the data by a user determined? Are criteria, procedures, controls, and responsibilities regarding access documented?**

FIPS 201 defines roles, and the role defines what access to data each user is provided.

<http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf>

**3) Will users have access to all data on the system or will the user's access be restricted? Explain.**

FIPS 201 defines roles, and the role defines what access to data each user is provided.

**4) What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those having access? (Please list processes and training materials)**

Federal Information Processing Standards 201 (FIPS 201) Personal Identity Verification (PIV) of Federal Employees and Contractors, NIST Standard 800-79, 800 – 53, and 800-37. defines roles, and the role defines what access to data each user is provided. FIPS are developed by National Institute Standards and Technology (NIST) in accordance with **Federal Information Security Management Act of 2002 ("FISMA", 44**



U.S.C. § 3541, *et seq.*). FIPS are approved by the Secretary of Commerce and are compulsory and binding for federal agencies. Since FISMA requires that federal agencies comply with these standards, agencies may not waive their use.

Guidance documents and recommendations are issued in the NIST Special Publication (SP) 800-series. Office of Management and Budget (OMB) policies (including OMB FISMA Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management) state that for other than national security programs and systems, agencies must follow NIST guidance.

FIPS 201, Recommended Security Controls for Federal Information Systems (SP 800-53), Guide for the Security Certification and Accreditation of Federal Information Systems (SP 800-37) defines a reliable, government-wide security controls to gain access to Federally controlled facilities and information systems, and developed within the context and constraints of Federal law, regulations, and policy based on information processing technology currently available and evolving.

- 5) **Are contractors involved with the design and development of the system and will they be involved with the maintenance of the system? If yes, were Privacy Act contract clauses inserted in their contracts and other regulatory measures addressed?**

The current system was integrated from several COTS products. Privacy Act contract clauses are referenced in NIST standards. Other regulatory measures were addressed, via inputting standard contract clauses.

- 6) **Do other systems share data or have access to the data in the system? If yes, explain.**

No.

- 7) **Who will be responsible for protecting the privacy rights of the public and employees affected by the interface?**

The PIV II system utilized is a turn key solution provided by a small disadvantaged (8(a) team. This team adhered to NIST standards throughout the integration process. The contractor system administrator, as well as the Privacy Officer, Chief Information Officer, and system role holders are all responsible for protecting the privacy rights of employees.

- 8) **Will other agencies share data or have access to the data in this system (Federal, State, and Local, Other (e.g., Tribal))?**

No.

- 9) **How will the data be used by the other agency?**

Not applicable.

**10) Who is responsible for assuring proper use of the data?**

Each action taken in the system is compiled in an audit log in the system. Each role holder's log on, activities, and log off the system are tracked. Only the System Administrator has access to these audit logs. Role holders do not have access to the system logs.

**G. PRIVACY IMPACT ANALYSIS**

- 1) Discuss what privacy risks were identified and how they were mitigated for types of information collected.

FIP 201 defines controls, which are built into the system. In addition to the standards of FIPS 201, SBA also recognized that the collection and display to each role holder is a privacy issue. In recognition of that Agency's standard operating procedure in which the Office of Inspector General which performs the adjudication function requires the full social security number, we masked all but the last four of the social security number to all other role holders.

<http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf>

- 2) Describe any types of controls that may be in place to ensure that information is used as intent.

Appropriate use of information covered as per FIPS 201. SBA is developing online training on the responsibilities of the role holders.

- 3) Discuss what privacy risks were identified and how they were mitigated for information shared internal and external?

Privacy risks:

The system process contains or digitally captures the following privacy items:

- Social security number
- Two forms of identification (as defined by Form 1-9)
- Biometric data
- Wrap sheet determination results

Privacy risks are minimized by implementing certain controls defined in FIP. These controls were built into the system. In addition to the standards of FIPS 201, SBA also recognized that the collection and display to each role holder is a privacy issue. In recognition of that Agency's standard operating procedure in which the Office of Inspector General which performs the adjudication function requires the full social

security number, we masked all but the last four of the social security number to all other role holders.

- 4) What privacy risks were identified and describe how they were mitigated for security and access controls?

Access to the system is restricted via system access controls:

- Party accessing the system must have a valid PIV card and enter the correct personal identification number (PIN)
- User name and assigned user privileges

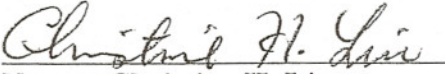
The system underwent a risk assessment in November, 2007. Vulnerabilities and Risks identified in the November 2007 assessment have been addressed. Once the system exits the pilot stage a Certification and Accreditation will be performed. The planned Certification and Accreditation is for the summer of 2008.

**See Attached Approval Page**

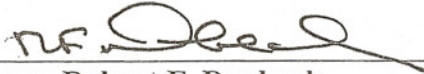


The Following Officials Have Approved this Document


1) System Co-Owner

 (Signature) 9/26/2008 (Date)  
Name: Christine H. Liu  
Title: Chief Information Officer and Privacy Officer

2) System Co-Owner

 (Signature) 9/26/08 (Date)  
Name: Robert F. Danbeck  
Title: Associate Administration  
For Management and Administration

3) Reviewing Official

 (Signature) 9/23/2008 (Date)  
Name: Herbert L. Mitchell  
Title: Associate Administration  
For Disaster Assistance

4) System IT Security Manager

 (Signature) 10/10/08 (Date)  
Name: David McCauley  
Title: Chief Information Security Officer