

## Privacy Impact Assessment

Federal Personal Identity Verification Identity Management System  
(PIV IDMS)

August 2007

## 1.1 DATA IN THE SYSTEM

Question	Explanation/Instructions/Response
<p>1. a. Describe all information to be included in the system, including personal data.</p>	<p>The information is collected from Personal Identity Verification (PIV) Applicants, the individuals to whom a PIV Card is issued. The PIV Applicant may be a current or prospective Federal employee or contractor. As required by FIPS 201, GSA will collect biographic and biometric information from the PIV Applicant in order to: (i) complete the identity proofing and registration process; (ii) create a data record in the PIV Identity Management System (IDMS); and (iii) issue a PIV Card.</p> <p>The personal information to be collected in the enrollment process will consist of data elements necessary to verify the identity of the individual and to perform background investigations concerning the individual. The PIV IDMS will collect data elements from the PIV Card applicant, including: name, date of birth, Social Security Number (SSN), organizational and employee affiliations, fingerprints, digital color photograph, work e-mail address, and phone number(s) as well as additional verification and demographic information.</p> <p>Other types of data contained in the system include military status; foreign national status; federal emergency response official status; law enforcement official status; results of a background check; and PIV Card issuance location. The FBI interface may require the following information which will be stored in the PIV IDMS: alias; gender; race; country and city of birth. Records in the PIV IDMS needed for credential management for enrolled individuals in the PIV Program include: PIV Card serial number (all past and current Card ID numbers are retained); digital certificate(s) serial number; PIV Card issuance and expiration dates; PIV Card personal identification number (PIN); Cardholder Unique Identification Number (CHUID); card management keys.</p> <p>System requirements also mandate the collection or generation of: an Applicant ID (Assigned); Method of Notification (Chosen); Ship to Address (Assigned by Sponsor); Government ID (Assigned based on Sponsor records); and Government Agency Code (Assigned based on Sponsor records).</p>
<p>1. b. What stage of the lifecycle is the system currently in?</p>	<p>The system is currently in a development phase. Full operational capability is anticipated to begin September 30, 2007.</p>
<p>2. a. What are the sources of the information in the system?</p>	<p>Information will come from official government Sponsors and Enrollment Officers (Registrars), who act on behalf of participating government agencies, as well as individual applicants. Information on pre-existing employees may also be batch imported into the system from participating government agencies HR systems.</p> <p>The PIV IDMS records will cover all participating Federal employees, contractors, and volunteers who require routine,</p>

	<p>long-term access to Federal facilities, IT systems, and networks. The system also includes individuals authorized to perform or use services provided in agency facilities (e.g., Credit Union, Fitness Center, etc.).</p> <p>It is the discretion of GSA and participating Federal agencies to include short-term (working in a Federal facility for less than six months) employees and contractors in the PIV Program and, therefore, inclusion in the PIV IDMS. Federal agencies shall make risk-based decisions to determine whether to issue PIV Cards and require prerequisite background checks for short-term employees and contractors.</p> <p>The system does not apply to occasional visitors or short-term guests. GSA and participating agencies will issue temporary identification and credentials for this purpose.</p>
2. b. What GSA files and databases are used?	The PIV IDMS will be used. This database is hosted at the Northrop Grumman data center in Chesterfield, Virginia.
2. c. What Federal agencies are providing data for use in the system?	<p>The PIV IDMS records will cover all participating agency employees, contractors, and volunteers who require routine, long-term access to Federal facilities, IT systems, and networks.</p> <p>Please reference the GSA Agency Shared Service Memorandum of Understanding (MOU) documentation for a detailed list of agencies.</p>
2. d. What State and local agencies are providing data for use in the system?	Currently, no State or local agencies provide data for use in this system.
2. e. What other third party sources will the data be collected from?	Data will not be collected from any other third-party sources.
2. f. What information will be collected from the individual whose record is in the system?	The personal information to be collected in the enrollment process will consist of data elements necessary to verify the identity of the individual and to perform background investigations concerning the individual. The data elements retained by the PIV IDMS for the PIV Card applicant include: name, date of birth, SSN, organizational and employee affiliations, fingerprints, digital color photograph, work e-mail address, and phone number(s), as well additional verification and demographic information. Other types of data contained in the system include: military status; foreign national status, federal emergency response official status; law enforcement official status; results of background check; and PIV Card issuance location.
3. a. How will the data collected from sources other than Federal agency records or the individual be verified for accuracy?	N/A.
3. b. How will data be checked for completeness?	The accuracy and completeness of the data is reviewed by key personnel at several stages: during the sponsorship process, during the enrollment process, and during the adjudication process.

	<p>The following technical controls also ensure the completeness of the data:</p> <ul style="list-style-type: none"> <li>• Consistency and reasonableness checks</li> <li>• Validation during data entry and processing</li> <li>• Use of required fields to prevent critical data from being omitted.</li> </ul>
<p>3. c. Is the data current? How do you know?</p>	<p>Yes, all data is considered current and is verified throughout the PIV Identity Proofing and Registration Process. It is first verified by the agency Sponsor, who submits the initial instance of an Applicant's biographic information within the system. During the enrollment process, a Registrar verifies and completes the Applicant's enrollment data contained in the system before submitting an enrollment record. An Adjudicator confirms the background check that every applicant must pass before being issued a credential.</p>
<p>4. Are the data elements described in detail and documented? If yes, what is the name of the document?</p>	<p>Yes, the data elements are described in detail, and are documented in the System Security Plan (SSP), Appendix D, Security Categorization..</p>

## 2.0 ACCESS TO THE DATA

Question	Explanation/Instructions/Response
<p>1. a. Who will have access to the data in the system?</p>	<p>Access to the data is strictly controlled, and is limited to those with an operational need to access the information. There are three core sets of user population:</p> <ol style="list-style-type: none"> <li>1. Users with administrative and operational responsibilities (e.g., Agency Security Officers) (hereinafter “administrative personnel”)</li> <li>2. Users who are provided access to the GSA MSO USAccess system and its applications (e.g., Sponsors, Registrars, and Adjudicators) (hereinafter “privileged users”)</li> <li>3. GSA MSO USAccess applicants (hereinafter “general users”).</li> </ol> <p>Administrative personnel and privileged users are subject to rigorous background checks before they are allowed access to the system.</p>
<p>1. b. Is any of the data subject to exclusion from disclosure under the Freedom of Information Act (FOIA)? If yes, explain the policy and rationale supporting this decision.</p>	<p>Yes. <u>5 U.S.C. 552(b)(6)</u>: sixth statutory exemption. GSA’s primary consideration in invoking the sixth statutory exemption under FOIA is protecting the privacy of the person who is the subject of a requested file. The public interest in disclosure must be balanced against personal privacy interests that may be invaded by disclosing the record. GSA will determine whether to release personal information under this exemption or when applying the personal privacy exemption for law enforcement records (5 U.S.C. 552(b)(7)(c)) by using a four step process:</p> <ol style="list-style-type: none"> <li>A. Is an identifiable personal privacy interest involved? If there is none, this exemption does not apply.</li> <li>B. Is a public interest involved: e.g., would disclosure benefit the general public in light of content and context of the information? If there is no general public interest to be served by disclosure, the personal information should be protected.</li> <li>C. Does the identified public interest qualify for consideration; e.g., is it an interest which would shed light on the agency’s performance of its statutory duties? If disclosure of requested information would not serve this interest, the personal privacy interest should be protected.</li> <li>D. Where an identifiable personal privacy interest and qualifying public interest are present, which is greater? If the privacy interest is greater, the information should be withheld. If the public interest is greater, this exemption does not apply.</li> </ol>
<p>2. How is access to the data by a user determined? Are criteria, procedures, controls, and responsibilities regarding access documented?</p>	<p>A “least-privilege” role-based access system restricts access to data on a “need-to-know” basis; access to the data is limited to those with an operational need to access the information. Users will be provided the GSA MSO USAccess <i>Operational Guide</i> and GSA MSO USAccess <i>PCI Operations Plan</i> to aide in</p>

	<p>accessing data within the system and understanding user responsibilities in handling accessed data.</p>
<p>3. Will users have access to all data in the system or will the user's access be restricted? Explain.</p>	<p>A "least-privilege" role-based access system restricts access to data on a "need-to-know" basis. Only a select few administrative and privileged users will have access to all the data, and these individuals undergo a rigorous background screening process. Accessing privileged functions also requires double- or triple-factor authentication.</p> <p>General users will only have access to their own data; again, this restriction is enforced by the role-based access system based on the defined user roles, and modification of this data is subject to approval by the "trusted administrator" user.</p>
<p>4. What controls are in place to prevent the misuse (e.g., browsing) of data by those having access?</p>	<p>All access has role-based restrictions, and individuals with access privileges have undergone vetting and suitability screening. All data exchange will take place over encrypted data communication networks. Private networks and/or encryption technologies will be used during the transfer of information to ensure that Internet "eavesdropping" does not take place and that data is sent only to its intended destination and to an authorized user, by an authorized user. Biometric image and template data is encrypted at rest and never issued in the clear. In addition, sensitive personal information such as SSN is encrypted or hashed at rest. GSA maintains an audit trail and performs random periodic reviews to identify unauthorized access. Persons given roles in the PIV process must be approved by the government and complete training specific to their roles to ensure they are knowledgeable about how to protect personally identifiable information.</p> <p>SSN information is available on the PIV card but is protected by the PIN and must be released by the user in any application.</p> <p>Furthermore, the system is fully compliant with FIPS 201, Part I (PIV-I), which describes the minimum requirements for a Federal personal identification system that meets the control and security objectives of HSPD-12. Ten requirements are listed in PIV-I stating how and to what extent "each agency's PIV implementation shall meet the four control objectives." FIPS 201 then specifies requirements for 1) PIV Identity Proofing and Registration (5 requirements); 2) PIV Issuance and Maintenance (4 requirements); and 3) PIV Privacy (10 requirements). The PIV Identity Proofing and Registration Requirements (FIPS 201 section 2.2) state, "The identity proofing and registration processes used when verifying the identity of the applicant shall be accredited by the department or agency as satisfying the requirements above and approved in writing by the head of the Federal department or agency."</p>
<p>5. a. Do other systems share data or have access to data in this system? If yes, explain.</p>	<p>Yes. Agencies purchasing services from GSA through the shared services solution will have access to their own agency data. An interface has been defined for agencies to connect to the SIP Web Services. The communication between agency and SIP is over an IPsec VPN which is secured and encrypted communication. Only authorized users can perform data operations.</p>

	<p>Also, the PKI and card-issuing systems will have access to the amount of data required to ensure that their services can be effectively provided. Access to this data will be restricted to a “need-to-know” basis. The communication to the PKI shared service provider is currently secured based on an SSL proxy solution. This communication link will be re-configured to be secured using a VPN SSL solution in the future.</p> <p>All data transfer to the card-issuing provider is done using FTP over SSL.</p>
<p>5. b. Who will be responsible for protecting the privacy rights of the individuals affected by the interface?</p>	<p>The GSA MSO Program Manager is responsible for protecting the privacy rights of the individuals affected by the interface. Furthermore, any individuals with a role identified or defined in the system GSA MSO USAccess <i>PCI Operations Plan</i> are also responsible for protecting the privacy rights of individuals (e.g., Sponsors, Registrars, Agency Privacy Officials).</p>
<p>6. a. Will other agencies share data or have access to data in this system (International, Federal, State, Local, And Other)?</p>	<p>No. Participating Federal agencies will only have access to their own particular agency’s data (not to any other agency’s data). The exception is disclosures generally permitted under 5 U.S.C. Section 552a(b) of the Privacy Act. All or a portion of the records or information contained in this system may be disclosed outside GSA as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:</p> <ul style="list-style-type: none"> <li>A. To the Department of Justice (DOJ) when: (a) The agency or any component thereof; or (b) any employee of the agency in his or her official capacity; (c) any employee of the agency in his or her individual capacity where agency or the Department of Justice has agreed to represent the employee; or (d) the United States Government, is a party to litigation or has an interest in such litigation, and by careful review, the agency determines that the records are both relevant and necessary to the litigation and the use of such records by DOJ is therefore deemed by the agency to be for a purpose compatible with the purpose for which the agency collected the records.</li> <li>B. To a court or adjudicative body in a proceeding when: (a) The agency or any component thereof; (b) any employee of the agency in his or her official capacity; (c) any employee of the agency in his or her individual capacity where agency or the Department of Justice has agreed to represent the employee; or (d) the United States Government, is a party to litigation or has an interest in such litigation, and by careful review, the agency determines that the records are both relevant and necessary to the litigation and the use of such records is therefore deemed by the agency to be for a purpose that is compatible with the purpose for which the agency collected the records.</li> <li>C. Except as noted on Forms SF 85, 85-P, and 86, when a record on its face, or in conjunction with other records, indicates a violation or potential violation of law, whether civil, criminal, or regulatory in nature, and whether arising by general statute or particular program statute, or by regulation, rule, or order issued pursuant thereto, disclosure may be made to the appropriate public authority, whether</li> </ul>

	<p>Federal, foreign, State, local, or tribal, or otherwise, responsible for enforcing, investigating or prosecuting such violation or charged with enforcing or implementing the statute, or rule, regulation, or order issued pursuant thereto, if the information disclosed is relevant to any enforcement, regulatory, investigative or prosecutorial responsibility of the receiving entity.</p> <ul style="list-style-type: none"><li>D. To a Member of Congress or to a Congressional staff member in response to an inquiry of the Congressional office made at the written request of the constituent about whom the record is maintained.</li><li>E. To the National Archives and Records Administration or to the General Services Administration for records management inspections conducted under 44 U.S.C. 2904 and 2906.</li><li>F. To agency contractors, grantees, or volunteers who have been engaged to assist the agency in the performance of a contract service, grant, cooperative agreement, or other activity related to this system of records and who need to have access to the records in order to perform their activity. Recipients shall be required to comply with the requirements of the Privacy Act of 1974, as amended, 5 U.S.C. 552a.</li><li>G. To a Federal agency, State, local, foreign, or tribal or other public authority, on request, in connection with the hiring or retention of an employee, the issuance or retention of a security clearance, the letting of a contract, or the issuance or retention of a license, grant, or other benefit, to the extent that the information is relevant and necessary to the requesting agency's decision.</li><li>H. To the Office of Management and Budget when necessary to the review of private relief legislation pursuant to OMB Circular No. A-19.</li><li>I. To a Federal State, or local agency, or other appropriate entities or individuals, or through established liaison channels to selected foreign governments, in order to enable an intelligence agency to carry out its responsibilities under the National Security Act of 1947, as amended, the CIA Act of 1949, as amended, Executive Order 12333 or any successor order, applicable national security directives, or classified implementing procedures approved by the Attorney General and promulgated pursuant to such statutes, orders or directives.</li><li>J. To an agency, organization, or individual for the purposes of performing authorized audit or oversight operations.</li><li>K. To the Office of Personnel Management in accordance with the agency's responsibility for evaluation of Federal personnel management.</li><li>L. To the Federal Bureau of Investigation for the FBI National Criminal History check.</li><li>M. To a Federal State, or local agency, or other appropriate entities or individuals, or through established liaison</li></ul>
--	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

	<p>channels to selected foreign governments, in order to enable an intelligence agency to carry out its responsibilities under the National Security Act of 1947 as amended, the CIA Act of 1949 as amended, Executive Order 12333 or any successor order, applicable national security directives, or classified implementing procedures approved by the Attorney General and promulgated pursuant to such statutes, orders or directives.</p>
<p>6. b. How will the data be used by the agency?</p>	<p>The information identified above is used in each step of the PIV process as described below:</p> <ol style="list-style-type: none"> <li>1. <u>Complete the identity proofing and registration process.</u> The biographic information collected or confirmed as part of this process is used to establish the PIV applicant's identity. Biometrics is used to accurately authenticate a PIV Applicant and to ensure he/she has not been previously enrolled in the PIV system. As part of this process, FIPS 201 requires that Applicants provide two forms of identity source documents in original form. The identity source documents must come from the list of acceptable documents included in Form I-9, OMB No. 115-0316, Employment Eligibility Verification.1 PIV Applicants will also participate in an electronic signature process conforming to the Electronic Signature (ESIGN) Act. This confirms presentation of and agreement with the privacy notice, confirms the intent to participate in the PIV process, and submission to a named-based threat background check as required depending on job requirements.</li> <li>2. <u>Create a data record in the PIV IDMS.</u> The PIV IDMS is used during the registration process to create the PIV Applicant's enrollment record, manage and maintain this information throughout the PIV Card lifecycle, and, verify, authenticate and revoke PIV Cardholder access to Federal resources. A unique identifier is assigned during registration and used to represent the individual's identity and associated attributes stored in the system.</li> <li>3. <u>Issue a PIV Card.</u> A PIV Card is issued upon successful completion of the enrollment process and successful background investigation. Biometrics is used during PIV Card issuance to verify PIV Applicant identity and complete activation of the card. This provides much stronger security assurances than typical card activation protections such as PINs and/or passwords. Once the individual has been issued a PIV Card, the PIV IDMS is updated to reflect that the card has been issued.</li> </ol>
<p>6. c. Who is responsible for assuring proper use of the data?</p>	<p>The GSA MSO PM is responsible for protecting the privacy rights of the individuals affected by the interface. Furthermore, any individuals with a role identified or defined in the system GSA MSO USAccess <i>PCI Operations Plan</i> are also responsible for protecting the privacy rights of individuals (e.g., Sponsors, Registrars, Agency Privacy Officials).</p>
<p>6. d. How will the system ensure that agencies only get the</p>	<p>The security architecture of the system, along with a strict role-based access program and user/role-based data partitioning,</p>

information they are entitled to?	will ensure that agencies only have access to the data to which they are authorized to access.
7. What is the life expectancy of the data?	<p>The active life expectancy of the data in the HSPD-12 PIV IDMS/CMS is for the duration of the active identity account, which could be for the duration of the individual's employment/assignment (for contractors) for shared service participating agencies.</p> <p>The GSA Records Retention Officer and the Department of Homeland Security developed the "GSA Personal Identity Verification IDMS Record Retention and Disposition Schedule" document for data retention schedules. As indicated, the retention requirements are a minimum of five years from the date when the identity account moves from an active to inactive status (month of separation).</p>
8. How will the data be disposed of when it is no longer needed?	Data will be disposed of according the requirements of NIST Special Publication (SP) 800-88 <i>Guidelines for Media Sanitization</i> . Magnetic media will be degaussed and then destroyed; paper records will be stored in locked bins, transported securely via bonded courier, and shredded.

### 3.0 ATTRIBUTES TO THE DATA

Question	Explanation/Instructions/Response
1. Is the use of the data both relevant and necessary to the purpose for which the system is being designed?	Yes. The data collected and used by the system is necessary to meet the requirements of HSPD-12, FIPS 201, and OMB M-05-24.
2. a. Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected?	No. While the inclusion of biometric data could be a new data element for some participants, nothing “new” can be learned about a person from the aggregation of data contained in the system. The sole purpose of the data contained in this system is to positively identify an individual—viewing all the data contained in this system would be the equivalent of viewing someone’s driver’s license and passport. (Also, it should be noted that many enrollees in this system have already provided their biometric—generally fingerprints—as part of their initial background screening check.)
2. b. Will the new data be placed in the individual's record (client or employee)?	N/A.
2. c. Can the system make determinations about individuals that would not be possible without the new data?	No. All of the data contained in the system is designed for one purpose only: to positively and accurately verify that a person is, in fact, who he/she claims to be.
2. d. How will the new data be verified for relevance and accuracy?	<p>The relevance of the data is verified by the requirements of HSPD-12 and FIPS 201—that is, the data collected is required to meet these federal requirements.</p> <p>The accuracy of the data is reviewed by key personnel during three stages: sponsorship process, enrollment process, and adjudication process.</p> <p>The following technical controls also ensure the accuracy of the data:</p> <ul style="list-style-type: none"> <li>• Consistency and reasonableness checks</li> <li>• Validation during data entry and processing</li> </ul> <p>The system uses a combination of the following to verify the integrity of data and look for evidence of data tampering, errors, and omissions:</p> <ul style="list-style-type: none"> <li>• Built-in auditing functionality</li> <li>• Data validation occurring before data is committed into the PIV IDMS</li> <li>• Using required fields to prevent critical data from being omitted.</li> </ul>
3. a. If the data is being consolidated, what controls are in place to protect the data and prevent unauthorized access? Explain.	<p>GSA MSO USAccess protects all records from unauthorized access through appropriate administrative, physical, and technical safeguards:</p> <p><u>System Security</u>: The controls include network security and limited access to system and physical facilities. These risks</p>

are addressed by the SSP and Risk Assessment established for this PIV Program. More specific program controls include protecting data through the use of FIPS validated cryptographic algorithms in transit, processing, and at rest.

Networks: The IT infrastructure that supports the PIV Program is described in detail in the SSP. 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 PIV IDMS. Access is PIN protected.

Data Transmission: All biographic and biometric data collected by the enrollment workstation is transmitted to the PIV IDMS over a private network in an encrypted format. In the condition that the enrollment center supports offline enrollments, all data files will be stored on the enrollment workstation in an encrypted format and will be automatically deleted from the workstation upon confirmation of a successful transmission. Auditable records are created for the transmission and successful deletion of enrollment records captured while working in an offline mode.

Data Storage Facilities: 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).

The PIV IDMS sends confirmed enrollment information to the card production facility via a secure FTP 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:

- **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 identification number (PIN), and/or biometric (e.g., fingerprint).

- 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 is 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.

Security of ID credential issued to an employee or contractor is achieved by full compliance with the mandatory requirements of the FIPS 201, *Personal Identity Verification of Federal Employees and Contractors*. Specific safeguards include:

- Card issuing authority limited to providers with official accreditation pursuant to NIST SP 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

	<ul style="list-style-type: none"> <li>• Employees are alerted to importance of protecting card</li> <li>• Card expiration within five years from issuance</li> <li>• Return of cards to agency when no longer needed (or upon employee/contractor separation from the agency)</li> <li>• Deactivation of card within 18 hours (the latest) of employee/contractor separation, loss of card, or expiration</li> <li>• Removal of all information in identifiable form (IIF) associated with the cardholder from the system upon deactivation if cardholder will not be reissued a new card</li> <li>• Specialized role-based training for all persons involved in the PIV process</li> </ul>
<p>3. b. If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? Explain.</p>	<p>See answer to 3a above.</p>
<p>4. How will the data be retrieved? Can it be retrieved by personal identifier? If yes, explain.</p>	<p>Before data can be retrieved, a user must positively and uniquely authenticate to the system, using a minimum of two-factor authentication; for some privileged types of access, three-factor authentication. The personal identifier required is a biometric. All system transactions are tied to a specific, unique individual by strict identification and authentication protocols, and there are audit trails that document which users perform which activities.</p>
<p>5. What are the potential effects on the privacy rights of individuals of:</p> <ol style="list-style-type: none"> <li>a. Consolidation and linkage of files and systems</li> <li>b. Derivation of data</li> <li>c. Accelerated information processing and decision making</li> <li>d. New technologies</li> <li>e. How are the effects to be mitigated</li> </ol>	<p>The effects are minimal. As stated earlier, the aggregation of the data contained in this system does not introduce any new privacy issues. While the inclusion of biometric data could be a new data element for some participants, nothing “new” can be learned about a person from the aggregation of data contained in the system.</p> <p>There are no new technologies being migrated.</p>

## 4.0 MAINTENANCE OF ADMINISTRATIVE CONTROLS

Question	Explanation/Instructions/Response
1. a. Explain how the system and its use will ensure equitable treatment of individuals.	The system is based on agency business processes. Any user who can participate in a government program, according to the laws governing the program, receives the same attention from the computer, and is processed under the same automated business rules as any other user.
1. b. If the system is operated in more than one site, how will consistent use of the system be maintained at all sites?	Enrollments into the PIV system will be conducted at identical sites across the network. A centrally managed training program is in place to support the standardization of the identity proofing and registration processes during this phase. The Registrars conducting the enrollments will also have access to Standard Operating Procedures and centrally managed help desk support. All system users must complete standardized training and use a consistent user interface.
1. c. Explain any possibility of disparate treatment of individuals or groups.	The system is based on agency business processes. Any user who can participate in a government program, according to the laws governing the program, receives the same attention from the computer, and is processed under the same automated business rules as any other user.
2. a. What are the retention periods of data in this system?	The GSA Records Retention Officer and the Department of Homeland Security developed the "GSA Personal Identity Verification IDMS Record Retention and Disposition Schedule" document for data retention schedules. As indicated, the retention requirements are a minimum of five years from the date when the identity account moves from an active to inactive status (month of separation). This document is located within the GSA MSO USAccess CM tool.
2. b. What are the procedures for eliminating the data at the end of the retention period? Where are the procedures documented?	The GSA Records Retention Officer and the Department of Homeland Security developed the "GSA Personal Identity Verification IDMS Record Retention and Disposition Schedule" document for data retention schedules. As indicated, the retention requirements are a minimum of five years from the date when the identity account moves from an active to inactive status (month of separation). This document is located within the GSA MSO USAccess CM tool.
2. c. While the data is retained in the system, what are the requirements for determining if the data is still sufficiently accurate, relevant, timely, and complete to ensure fairness in making determinations?	The requirement is not for data accuracy "to ensure fairness in making determinations". This is actually a Privacy Act requirement to ensure that data that is being retained in the Federal Systems of Records is accurate. See the GSA System of Records Notice (SORN) for the justification for data relevancy and retention. For ongoing data accuracy, the data must be reviewed by the sponsor/card holder at least every five years for accuracy at time of re-issuance. Further, cardholders are trained to provide data updates so the ongoing PIV IDMS/CMS/card data records are accurate.

<p>3. a. Is the system using technologies in ways that Federal agencies have not previously employed (e.g., Caller-ID)?</p>	<p>HSPD-12 requires the use of biometric data, contained on a "smart card," to positively identify an individual requiring access to a government facility or computer system. The use of biometric-based smart cards on such a scale is a relatively new endeavor for Federal agencies. However, the use of identification cards and badges to positively identify an authorized individual is not new at all</p>
<p>3. b. How does the use of this technology affect individuals' privacy?</p>	<p>The use of this system does not really affect an individual's privacy, as all the data contained on the card and in the system has almost certainly already been provided during the course of employment application, security background screening, and badge issuance. In fact, one could make a very solid argument that this system actually <i>protects</i> privacy, as the use of a USAccess Program identity card greatly reduces the chance of someone using a government-issued credential to falsely claim someone else's identity.</p>
<p>4. a. Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.</p>	<p>No. Personal information, such as phone, address, and email, is available to contact personnel but NO MONITORING OF LOCATION is embedded in the system.</p>
<p>4. b. Will this system provide the capability to identify, locate, and monitor groups of people? If yes, explain.</p>	<p>No.</p>
<p>4. c. What controls will be used to prevent unauthorized monitoring?</p>	<p>The GSA MSO USAccess system maintains a strong security posture and network security to protect Personal Identifiable Information (PII) by the inherent security of the system (i.e., firewalls, passwords, cryptographic logon, and separation of roles). The system is a repository of identity information and has no access to the location of personnel or their movements and is not capable of monitoring system or building access.</p>
<p>5. a. Under which Privacy Act System of Records notice (SOR) does the system operate? Provide number and name.</p>	<p>This system operates under the SORN entitled the Federal "Personal Identity Verification Identity Management System (PIV IDMS)." (SORNs can be viewed at <a href="http://www.access.GPO.gov">www.access.GPO.gov</a>)</p> <ul style="list-style-type: none"> <li>• GSA/GOVT-7</li> </ul>
<p>5. b. If the system is being modified, will the SORN require amendment or revision? Explain.</p>	<p>No.</p>