USAccess

Privacy Impact Assessment (PIA)

August 3, 2020

POINT *of* CONTACT

Richard Speidel

gsa.privacyact@gsa.gov

Chief Privacy Officer
GSA IT
1800 F Street NW
Washington, DC 20405

Stakeholders

Name of Information System Security Manager (ISSM):

- Arpan Patel

Name of Program Manager/System Owner:

- Darlene Gore

Signature Page

Signed:

DocuSigned by:
Arpan Patel
8B059AABDAF1477...

Information System Security Manager (ISSM)

DocuSigned by:
Darlene Gore
4DFA92311ABF40E...

Program Manager/System Owner

DocuSigned by:
Richard Speidel
171D5411183F40A...

Chief Privacy Officer (CPO) - Under the direction of the Senior Agency Official for Privacy (SAOP), the CPO is responsible for evaluating the PIA and ensuring the program manager/system owner has provided complete privacy-related information.

Document Revision History

Date	Description	Version of Template
02/05/2019	Initial version of PIA under USAccess core services contract award from 2017. Based on GSA PIA template version 2.4 dated November 28, 2018. Authored and reviewed by the GSA MSO and Perspecta (Enterprise Services, LLC).	2.4
07/17/2020	Annual revision. Based on GSA PIA template version 3.1 dated February 20, 2020. Updated and reviewed by the GSA MSO and Perspecta.	3.1

Table of contents

6.1 Who or what will have access to the data in the project? What is the authorization process for access to the project?

6.2 Has GSA completed a system security plan (SSP) for the information system(s) supporting the project?

6.3 How will the system be secured from a physical, technical, and managerial perspective?

6.4 Are there mechanisms in place to identify and respond to suspected or confirmed security incidents and breaches of PII? If so, what are they?

SECTION 7.0 INDIVIDUAL PARTICIPATION

7.1 What opportunities do individuals have to consent or decline to provide information? Can they opt-in or opt-out? If there are no opportunities to consent, decline, opt in, or opt out, please explain.

7.2 What procedures allow individuals to access their information?

7.3 Can individuals amend information about themselves in the system? If so, how?

SECTION 8.0 AWARENESS AND TRAINING

8.1 Describe what privacy training is provided to users, either generally or specifically relevant to the project.

SECTION 9.0 ACCOUNTABILITY AND AUDITING

9.1 How does the system owner ensure that the information is being used only according to the stated practices in this PIA?

Document purpose

This document contains important details about *[system, application, or project]*. To accomplish its mission *[GSA office]* must, in the course of *[program name]*, collect personally identifiable information (PII) about the people who use such products and services. PII is any information[1] that can be used to distinguish or trace an individual's identity like a name, address, or place and date of birth.

GSA uses Privacy Impact Assessments (PIAs) to explain how it collects, maintains, disseminates, uses, secures, and destroys information in ways that protect privacy. This PIA comprises sections that reflect GSA's privacy policy and program goals. The sections also align to the Fair Information Practice Principles (FIPPs), a set of eight precepts codified in the Privacy Act of 1974.[2]

A. System, Application, or Project Name:

USAccess

B. System, application, or project includes information about:

Federal employees and contractors.

C. For the categories listed above, how many records are there for each?

Approximately 1.8 million records about unique federal employees and contractors as of 2020.

D. System, application, or project includes these data elements:

USAccess enables agency customers to collect and store, in the USAccess system, the following data, in support of HSPD-12 compliant PIV credential issuance and maintenance:

- *Name and other biographic, demographic or biometric information (date of birth, age, gender, height, weight, eye color, hair color, fingerprints, facial image);*
- *Contact information (address, telephone number, email address);*
- *Social Security Number (SSN), Driver's license number, passport number, or other government-issued identifiers or images of documents;*

Overview

USAccess is a shared Personal Identity Verification (PIV) credential issuance and maintenance service, supporting over 100 federal agencies that enables those agencies to issue secure, reliable identity credentials based on Public Key Infrastructure certificates, that are compliant

with Homeland Security Presidential Directive 12 (HSPD-12). These credentials are used for logical and physical access to federal information systems and facilities.

GSA collects biographic and biometric information from PIV applicants 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 and maintain a PIV Card with PKI certificates (from a third party provider) using a Card Management System (CMS).

The GSA Managed Service Office (MSO), in coordination with customer agencies, operates USAccess as an enterprise-class, cost efficient, system, and shared service, that offers best-in-class value for the U.S. Government and American people. USAccess is a mature, production, system that has serviced the federal government for over 10 years.

As described in System of Records Notice (SORN) 80 FR 64416, enrollment records maintained in the PIV IDMS on individuals applying for the PIV program and a PIV credential through the GSA HSPD-12 managed service include the following data fields: Full name; Social Security Number; Applicant/Enrollment ID number (system generated), date of birth; current address; digital color photograph; biometric templates (fingerprints); organization/office of assignment; employee affiliation; personal and work email addresses; work telephone number(s); office address; copies of identity source documents; employee status; military status; foreign national status; federal emergency response official status; law enforcement official status; results of background check; Government agency code; and PIV card issuance location. Records in the PIV IDMS and/or Credential/Card Management System needed for credential management for enrolled individuals in the PIV program include: PIV card serial number; digital certificate(s) serial number; PIV card issuance and expiration dates; PIV card PIN; Cardholder Unique Identifier (CHUID); and card management keys. Agencies may also choose to collect the following data at PIV enrollment which would also be maintained in the PIV IDMS: Physical characteristics (e.g., height, weight, and eye and hair color). Individuals enrolled in the PIV managed service will be issued a PIV card. The PIV card contains the following mandatory visual personally identifiable information: Name, photograph, employee affiliation, organizational affiliation, PIV card expiration date, agency card serial number, and color-coding for employee affiliation. Agencies may choose to have the following optional personally identifiable information printed on the card: Cardholder physical characteristics (height, weight, and eye and hair color). The card also contains an integrated circuit chip which is encoded with the following mandatory data elements which comprise the standard data model for PIV logical credentials: PIV card PIN, cardholder unique identifier (CHUID), PIV authentication digital certificate, and two fingerprint biometric templates. The PIV data model may be optionally extended by agencies to include the following logical credentials: Digital certificate for digital signature, digital certificate for key management, card authentication keys, and card management system keys. All PIV logical credentials can only be read by machine.

Information comes from official government Sponsors and Enrollment Officers (Registrars), who act on behalf of participating government agencies, as well as individual PIV applicants. Information on pre-existing employees may also be "batch" imported into the system from participating government agencies HR systems.

IDMS records cover all participating agency employees, contractors and their employees, consultants, and volunteers who require routine, long-term access to federal facilities, information technology 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.). At their discretion, participating Federal agencies may include short-term employees and contractors in the PIV program and, therefore, inclusion in the 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.

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.

SECTION 1.0 PURPOSE OF COLLECTION

GSA states its purpose and legal authority before collecting PII.

1.1 What legal authority and/or agreements allow GSA to collect, maintain, use, or disseminate the information?

The primary authorities that allow the GSA to collect the aforementioned information include:

- *Homeland Security Presidential Directive 12 (HSPD-12): Policy for a Common Identification Standard for Federal Employees and Contractors*

- *FIPS 201-2: Personal Identity Verification (PIV) of Federal Employees and Contractors*

- *Interagency Agreements (IAAs) - Agreements signed with each agency participating in the shared service*

1.2 Is the information searchable by a personal identifier, for example a name or Social Security Number? If so, what System of Records Notice(s) apply/applies to the information?

As described in the SORN: GSA/GOVT-7, records may be retrieved by name of the individual, Cardholder Unique Identification Number, Enrollment ID, Social Security Number, and/or by any other unique individual identifier.

1.3 Has an Information Collection Request (ICR) been submitted to or approved by the Office of Management and Budget (OMB)? If yes, provide the relevant names, OMB control numbers, and expiration dates.

No. An ICR has not been submitted for USAccess.

1.4 Has a records retention schedule been approved by the National Archives and Records Administration (NARA)? Explain how long and for what reason the information is retained.

The active life expectancy of the data in the HSPD-12 USACCESS IDMS/ Card Management System (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.

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).

Disposition of records will be according to NARA disposition authority N1-269-06-1 (pending).

SECTION 2.0 OPENNESS AND TRANSPARENCY

GSA is open and transparent. It notifies individuals of the PII it collects, maintains, uses or disseminates as well as how it protects and shares it. It provides straightforward ways for individuals to learn how GSA handles PII.

2.1 Will individuals be given notice before the collection, maintenance, use or dissemination of personal information about themselves? If not, please explain.

GSA requires that customer agencies display (post) a Privacy Act Notice in credentialing centers. Also, PIV card applicants are required to digitally sign an acknowledgement statement when they receive their PIV card. The following text is in both the posted notice and the digital acknowledgement:

PRIVACY ACT STATEMENT

AUTHORITY: E.O. 9397. PRINCIPAL PURPOSE(S): To collect social security number and other personal identifiers during the certification registration process, to ensure positive identification of the subscriber who signs this form. ROUTINE USES: Information is used in the PIV registration process. DISCLOSURE: Voluntary; however, failure to provide the information may result in denial of issuance of a token containing PKI private keys. You have been authorized to receive one or more digital credentials (PKI certificates) associated with private and public key pairs contained on your PIV card.

At a minimum, these key pairs enable you to electronically identify yourself for systems access. Additional key pairs may enable you to digitally sign documents and messages and perform encryption/decryption functions.

Upon pressing or clicking on the "I Agree" button, you will be asked to present the Personal Identification Number (PIN) that you selected just prior to the appearance of this acknowledgement form.

You are digitally signing this acknowledgement statement, which is legally binding, in lieu of a written signature. Acknowledgement of Responsibilities:

SECTION 3.0 DATA MINIMIZATION

GSA limits PII collection only to what is needed to accomplish the stated purpose for its collection. GSA keeps PII only as long as needed to fulfill that purpose.

3.1 Why is the collection and use of the PII necessary to the system, application, or project?

The identity proofing documents collected by USAccess operators and stored in the USAccess system is necessary to meet the identity proofing standards outlined in FIPS 201-2. Further, much of the PII (e.g. biometrics) collected is necessary for production of the PIV card, in accordance with federal standards. USAccess customers rely on these credentials to identify their employees and contractors in order to provide those individuals with logical and physical access to agency information systems and facilities.

3.2 Will the system, application, or project create or aggregate new data about the individual? If so, how will this data be maintained and used?

No. The USAccess program and system will neither aggregate previously unavailable data about an individual, nor will it create new data about an individual. USAccess operators are trained in

and provided written guidance detailing the acceptable forms and quantity of identification to identity PIV applications in the enrollment process. Additionally, the USAccess system applies appropriate minimization rules to prevent unnecessary data on specific individuals from being collected. For example, the system will only ask for and accept, as scanned copies, the number of identity documents required to meet the identity proofing standards in FIPS 201-2.

3.3 What protections exist to protect the consolidated data and prevent unauthorized access?

USAccess protects personal information relevant to PIV applicants and cardholders as described in Section 6, Security, below.

3.4 Will the system monitor the public, GSA employees, or contractors?

The USAccess system does not have the capability to geographically locate or monitor individuals, apart from audit logging of functions performed by USAccess operators with role-holder accounts. This is only done in accordance with IT Security requirements and described by the "Warning banner" these individuals acknowledge when logging onto the system.

3.5 What kinds of report(s) can be produced on individuals?

USAccess has many built-in reports that are available to designated role-holders among the federal agencies that make use of the shared service. Agency role-holders only have scope within USAccess to view reports containing to PIV issuance data for the employees and contractors of their agency. Reports may include any PII data element stored in the IDMS, except SSN, facial images, and scanned identity documents. All system generated reports included a privacy/PII warning.

3.6 Will the data included in any report(s) be de-identified? If so, what process(es) will be used to aggregate or de-identify the data?

None of the reports available in USAccess that contain PII for specific individuals use any processes to de-identify and/or aggregate these data.

SECTION 4.0 LIMITS ON USING AND SHARING INFORMATION

GSA publishes a notice about how it plans to use and share any PII it collects. GSA only shares PII in ways that are compatible with the notice or as stated in the Privacy Act.

4.1 Is the information in the system, application, or project limited to only the information that is needed to carry out the purpose of the collection?

The USAccess system only collects personally identifiable information that is required for the issuance and maintenance of Personal Identification Verification (PIV) or PIV-Interoperable (PIV-I) credentials according to the Federal Information Processing Standard (FIPS) 201-2 and NIST Special Publication 800-79. The PII collected includes biographic and biometric information about a PIV or PIV-I applicant that is required to satisfy identity-proofing requirements for the issuance and maintenance of PIV or PIV-I credentials, including Full Name, Date of Birth, Social Security Number, Government Agency Affiliation, E-Mail Address, Facial Image, Fingerprints, and two forms of identity-proofing documents.

The USAccess system ensures that the information collected will only be used in ways that are compatible with the purpose for which the PII was collected through the use of role-based access controls. The PII is only accessible to Role Holders or Administrative personnel within the system who use a PIV credential to authenticate to the system (multi-factor authentication). Role Holders are Government Agency personnel who have been issued a PIV credential and who are granted PIV issuance and maintenance roles (i.e. Sponsor, Registrar, Activator, Adjudicator) by their respective agency. The system further segregates access by Role Holders to the information logically by Government Agency and Sub-Agency/Bureau affiliation. Administrative personnel are government contractors who have been issued a PIV credential by GSA, who deliver and maintain the PIV issuance system/service for GSA, and who have privileged access to the USAccess system for operations, maintenance, and troubleshooting purposes.

4.2 Will GSA share any of the information with other individuals, federal and/or state agencies, or private-sector organizations? If so, how will GSA share the information?

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:

- *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.

- *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.*
- *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 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.*
- *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.*
- *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.*
- *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.*
- *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.*
- *To the Office of Management and Budget (OMB) when necessary to the review of private relief legislation pursuant to OMB Circular No. A-19.*

- *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.*
- *To an agency, organization, or individual for the purposes of performing authorized audit or oversight operations.*
- *To the Office of Personnel Management in accordance with the agency's responsibility for evaluation of Federal personnel management.*
- *To the Federal Bureau of Investigation for the FBI National Criminal History check.*
- *To appropriate agencies, entities, and persons when (1) the Agency suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (2) the Agency has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by GSA or another agency or entity) that rely upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with GSA's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.*

4.3 Is the information collected directly from the individual or is it taken from another source? If so, what is the other source(s)?

Information comes from official government Sponsors and Enrollment Officers (Registrars), who act on behalf of participating government agencies, as well as individual PIV applicants. Information on pre-existing employees may also be batch imported into the system from participating government agencies HR systems.

The USAccess IDMS records cover all participating Federal employees, contractors, and volunteers who require routine, 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.).

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 USAccess 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.

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.

4.4 Will the system, application, or project interact with other systems, applications, or projects, either within or outside of GSA? If so, who and how? Is a formal agreement(s) in place?

Yes. Agencies purchasing services from GSA through the shared services solution will have access to their own agency data. Access is directly by individual role-holders (authorized system users) or a System Infrastructure Provider (SIP) Web Services interface that has been defined for agencies to connect HR and related systems for sharing PIV applicant and cardholder data. The communication between agency and the USAccess SIP interface is over a mutually authenticated, encrypted, Hypertext Transfer Protocol Secure (HTTPS) connection. Only authenticated (issued a certificate) and authorized (each agency is only authorized access to their data) system interfaces can perform data operations. Memorandums of Agreement (MOA) are signed with each agency that participates in this service. The MOA describes incident reporting responsibilities for each agency.

Also, the USAccess system interfaces with multiple Public Key Infrastructure (PKI) certificate authorities (CAs) for the issuance of PKI certificates to be encoded on PIV and PIV-I cards. These include the Entrust Managed Services SSP CA, the Entrust Non-Federal Issuers CA, the Treasury Operational CA and the Veteran's Affairs (VA) CA. The communication with these CA providers are secured using a Virtual Private Network connection. PIV applicant name and organizational affiliation data are transmitted to these service providers. The Entrust Managed Services SSP CA and the Entrust NFI CA undergo Security Assessment and Authorization by the GSA, are issued an Authority to Operate (ATO), and are subject to the GSA's incident reporting policies and procedures. The Treasury Operational CA undergoes Security Assessment and Authorization by the Treasury Department, are issued an Authority to Operate (ATO), and are subject to the Treasury Department's incident reporting policies and procedures. The VA CA undergoes Security Assessment and Authorization by the VA, are issued an Authority to Operate (ATO), and are subject to the VA's incident reporting policies and procedures.

Data also is transferred to a GSA-contracted commercial smart card printing/personalization provider over a secure File Transfer Protocol (SFTP) connection. PIV applicant name, agency affiliation, facial image, height, eye color, hair color, and employee/contractor status data are exchanged with this provider.

Data also is transferred to the Office of Personnel Management/Defense Counterintelligence and Security Agency over a secure Virtual Private Network connection. PIV applicant biographic and biometric (fingerprint) data are transmitted to this provider to facilitate Agency background investigation processes.

SECTION 5.0 DATA QUALITY AND INTEGRITY

GSA makes reasonable efforts to ensure that all PII it maintains is accurate, relevant, timely, and complete.

5.1 How will the information collected, maintained, used, or disseminated be verified for accuracy and completeness?

Initial information regarding a PIV applicant is provided through an agency sponsor. This information establishes an identity record for the individual and they subsequently complete an "enrollment," during which, biographic and biometric information is collected.

The biographic information collected or confirmed as part of this process is used to establish the PIV applicant's identity. Biometrics are used to authenticate a PIV applicant and to ensure he/she has not been previously enrolled in the USAccess system. As part of this process, FIPS 201-2 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.

The accuracy of the data is reviewed by key personnel during three stages: sponsorship process, enrollment process, and adjudication process.

The following technical controls also ensure the accuracy of the data:

- *Consistency and reasonableness checks*
- *Validation during data entry and processing*

The system uses a combination of the following to verify the integrity of data and look for evidence of data tampering, errors, and omissions:

- *Built-in auditing functionality*

- *Data validation occurring before data is committed into the USAccess IDMS*
- *Using required fields to prevent critical data from being omitted.*

SECTION 6.0 SECURITY

GSA protects PII from loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.

6.1 Who or what will have access to the data in the system, application, or project? What is the authorization process to gain access?

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:

- *Users with administrative responsibilities for system operation and maintenance of the USAccess infrastructure (e.g., System and Database Administrators).*
- *Users with privileged USAccess application access (e.g. System and Agency Security Officers)*
- *USAccess Application Role Holders (i.e. non-privileged users) who are provided access to the USAccess application for carrying out role-specific functions in the PIV issuance and maintenance lifecycle (e.g., Sponsors, Registrars, and Adjudicators)*

Administrative personnel and privileged users are subject to rigorous background checks before they are allowed access to the system. Access for Application Role Holders is granted and managed by Role Administrators for each customer agency. Access for administrative users is managed by Perspecta, with access being terminated when a user transfers from the USAccess support organization.

A "least-privilege" role-based access system is employed that 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. Additionally, all web-based access to the applications for PIV issuance and maintenance functions require PIV-based Multi-Factor Authentication (MFA).

6.2 Has GSA completed a System Security Plan (SSP) for the information system(s) or application?

USAccess has maintained a System Security Plan (SSP) and a FISMA ATO for over 10 years. The current ATO was issued on March 1, 2019.

6.3 How will the system or application be secured from a physical, technical, and managerial perspective?

USAccess protects all records from unauthorized access through appropriate administrative, physical, and technical safeguards:

System Security: The controls include network security and limited access to system and physical facilities. These risks 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.

Data Transmission: All biographic and biometric data collected by the enrollment workstation is transmitted to the USAccess IDMS over an encrypted channel. Auditable records are created for the transmission of enrollment records.

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.

Equipment:

- *User Identification: System Role Holders use PIV cards to authenticate to the system.*
- *User Access Control: 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. 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 encryption in transit, at rest, and at the database level.*
- *Audit Trails: System operations and events are recorded in various audit logs*
- *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 (customer agency responsibility), data center 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 system equipment.

- *A periodic assessment of technical, administrative, and managerial controls to ensure compliance of security controls, data integrity, and accountability, is performed triannually.*
- *Application Role Holders complete training associated with their specific role(s) in the PIV issuance and maintenance processes.*

6.4 Are there mechanisms in place to identify and respond to suspected or confirmed security incidents and breaches of PII? If so, what are they?

In accordance with NIST standards and GSA IT Security policies, the USAccess environment, including boundary access points and internal system assets and communication are subject to auditing and monitoring to identify anomalous activity. System reports are available to customer agencies to assist them in identifying risks associated with individual applicants/card holders (e.g. expired credentials that without a record of physical destruction). If a suspected or confirmed incident occurs, USAccess maintains an Incident Response Plan (IRP) in accordance with GSA IT Security policy. Mechanisms and procedures for conducting incident response (including suspected or confirmed breaches of PII) are detailed in the IRP, which is tested on an annual basis. Incidents occurring in customer-operated credentialing centers are subject to their respective agency policies, however, customers are also obligated through Inter-Agency Agreements and the USAccess RPS, to notify the GSA MSO, in the event that an incident occurs involving USAccess. Additionally, agencies that participate in our SIP web service offering are obligated to reporting standards that align with GSA IT Security policies, through the SIP MOA that is signed between the GSA and the customer agency.

USAccess has also participated in an Annual Breach Response Exercise with the GSA Privacy Office.

SECTION 7.0 INDIVIDUAL PARTICIPATION

GSA provides individuals the ability to access their PII and to correct or amend it if it is inaccurate. If GSA exempts a system or program from access, amendment and other provisions of the Privacy Act, it notifies the public of that exemption.

7.1 What opportunities do individuals have to consent or decline to provide information? Can they opt-in or opt-out? If there are no opportunities to consent, decline, opt in, or opt out, please explain.

As PIV is a common identity standard required in the federal government, individuals may decline to provide information, but in doing, will forego their ability to obtain a PIV credential.

Depending on agency policy and usage scenarios, "opting out" may also result in the inability to be employed by their sponsoring agency.

7.2 What procedures allow individuals to access their information?

Pursuant to the GSA procedures for an individual accessing their information stored in USAccess and in accordance with GSA's Privacy Act Rules, a PIV applicant/card holder that does not have direct access to their information may coordinate with a Sponsor or other authorized role holder in their respective agency to obtain a report. An individual in an agency other than the GSA can also petition the GSA to obtain this information from a role holder within the GSA MSO.

7.3 Can individuals amend information about themselves? If so, how?

A USAccess card-holder generally does not have the ability to directly access or modify information on themselves. If a card-holder becomes aware of information that is inaccurate or otherwise needs to be amended (a name change, e.g.) they can work through their agency sponsor to have the issue addressed. Certain updates are able to be made on existing PIV cards, while others may require re-print of the card or possibly re-enrollment (to ensure that identity proofing standards are maintained).

SECTION 8.0 AWARENESS AND TRAINING

GSA trains its personnel to handle and protect PII properly.

8.1 Describe what privacy training is provided to users, either generally or specifically relevant to the system, application, or project.

The GSA requires all GSA staff to complete privacy and security training. Similarly, the USAccess vendor, Perspecta, requires all administrative users to complete corporate-sponsored security awareness and privacy training annually.

The USAccess program also requires all system role-holders (including from customer agencies) to complete role-specific training, including measures to properly handle and maintain sensitive information, including PII,, associated with their role. Role-holders are not permitted access to the system until training has been completed. All training is tracked in the system. Periodic "refresher" training is offered, as necessary.

SECTION 9.0 ACCOUNTABILITY AND AUDITING

GSA's Privacy Program is designed to make the agency accountable for complying with the Fair Information Practice Principles. GSA regularly checks that it is meeting the requirements and takes appropriate action if it is not.

9.1 How does the system owner ensure that the information is used only according to the stated practices in this PIA?

As a government-wide shared service, USAccess relies on agency customers to maintain certain compliance objectives, adhere to certain standards, and assist in maintaining the PIV issuance service in accordance with the practices herein. The USAccess system employs technical controls, where and when possible, to ensure data integrity, enforce standards, and limit available functions to ensure compliance. Technical controls include but are not limited to data validation, read-only access (where appropriate), role-based access control, etc.

The USAccess program and system are subject to the following audit and accountability processes conducted by third-party organizations:

- *Tri-annual FISMA Security Assessment and Authorization (SA&A)*
- *Tri-annual PIV Card Issuers (PCI) Assessment and Authorization*
- *Annual Federal PKI audit (registration practices)*

---

[1] OMB Memorandum *Preparing for and Responding to the Breach of Personally Identifiable Information* (OMB M-17-12) defines PII as: "information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual." The memorandum notes that "because there are many different types of information that can be used to distinguish or trace an individual's identity, the term PII is necessarily broad."

[2] Privacy Act of 1974, 5 U.S.C. § 552a, as amended.