Privacy Impact Assessment for the VA IT System called:

NextGen PIV Assessing

VA Central Office (VACO)

Office of Identity, Credentialing, and Access Management

eMASS ID # 0158

Date PIA submitted for review:

July 31, 2024

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Julie Drake	Julie.Drake@va.gov OITPrivacy@va.gov	202-632-8431
Information System Security Officer (ISSO)	Anita Feiertag	Anita.Feiertag@va.gov	513-289-8116
Information System Owner	Reed Meyer	Reed.Meyer@va.gov	240-500-5904

Abstract

The abstract provides the simplest explanation for "what does the system do?".

NextGen Personal Identification Verification (PIV) uses General Services Administration's (GSA's) USAccess system and relies on a reciprocal Authority to Operate (ATO) agreement. NextGen PIV has no control over data or systems. Veterans Administration (VA) users connect to GSA USAccess using Hypertext Transfer Protocol Secure (HTTPS).

The GSA manages the NextGen PIV USAccess system, which is used to issue Homeland Security Presidential Directive 12 (HSPD-12) compliant PIV cards to VA employees, contractors, and affiliates. This is a non-persistent connection with an external government agency. The VA does not manage security requirements on GSA's side of the firewall. The connection from the VA sends Personally Identifiable Information (PII) data, no health information, via the VA Trusted Internet Connection (TIC) on Port 443 with Transport Layer Security (TLS) 1.2 encryption to GSA/USAccess. GSA/USAccess is responsible for maintaining the security controls and documentation of their system. The VA sends an approved reviewer to audit GSA/USAccess to ensure their compliance with securing data they maintain for the VA.

Overview

The overview is the most important section of the PIA. A thorough and clear overview gives the reader the appropriate context to understand the responses in the PIA. The overview should contain the following elements:

1 General Description

A. What is the IT system name and the name of the program office that owns the IT system?

System Name: Next Generation Personal Identity Verification (NextGen PIV)
Program Office: Office of Identity, Credentialing, and Access Management

B. What is the business purpose of the program, IT system, or technology and how it relates to the program office and agency mission?

NextGen PIV uses the General Services Administration's (GSA's) USAccess system. 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 (PKI) 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.

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.

C. Who is the owner or control of the IT system or project?

The system is owned by Office of Operational Security and Preparedness (OSP), Homeland Security Presidential Directive 12 (HSPD-12) Program Office.

2. Information Collection and Sharing

D. What is the expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual?

The USAccess application implemented by NextGen PIV contains biographic and identity data required for federal government employees, contractors, and affiliated to be issued a personal identity verification (PIV) card. USAccess contains data for approximately 2.5 million records across all federal agencies using the system, of which approximately 900,000 are current or former VA staff members.

E. What is a general description of the information in the IT system and the purpose for collecting this information?

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 Private Key Infrastructure (PKI) certificates (from a third-party provider) using a Card Management System (CMS). Information is entered by credentialed government Sponsors and Enrollment Officers (Registrars), who act on behalf of participating government agencies, as well as individual PIV applicants.

F. What information sharing conducted by the IT system? A general description of the modules and subsystems, where relevant, and their functions.

NextGen PIV does not contain any subsystems. PII data within sponsorship, adjudication, and enrollment modules are only visible to trained and privileged VA sponsor, adjudicator, and registrar role holders. The USAccess service is managed by the General Service Administration.

G. Is the system is operated in more than one site, and if so, a description of how use of the system and PII is maintained consistently in all sites and if the same controls are used across sites?

NextGen PIV employs the General Services Administration's (GSA) USAccess PIV Card Management Solution, which uses an on premise solution. The data center locations are:

- GSA USAccess Primary Data Center:
  250 Burlington Drive
  Clarksville, VA 23927-3201
- GSA USAccess Recovery Data Center:
  311 Rockrimmon Blvd. South
  Colorado Springs, CO 80919

The system will be used at all approved VA PIV Issuing Facilities, of which there are currently 234. The deployment of the system is standard across all sites and underlying workstations based on an approved IT image that has undergone full intake, testing, and

deployment with VA Device and Desktop Engineering (DDE) and Client Technologies (CT). The following ensure consistent PII maintenance across all sites:

- PIV issuing facilities must undergo a standard authorization and accreditation process with the Office of Operational Security and Preparedness (OSP), Homeland Security Presidential Directive 12 (HSPD-12) Program Office prior to approval to begin PIV issuance activities.
- Personnel request to have system roles assigned that allow access to PII must complete training and submit completed training certificates to the Office of Operational Security and Preparedness (OSP), Homeland Security Presidential Directive 12 (HSPD-12) Program Office

3. Legal Authority and SORN

H. What is the citation of the legal authority to operate the IT system?

- Homeland Security Presidential Directive 12 (HSPD-12), C.F.R. 2014 Title 32, Vol.1, §161-4
- National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) 201-2: Personal Identity Verification (PIV) of Federal Employees and Contractors, §2.1-2.11
- System of Records Notice (SORN)
  - 146VA005Q3/73 FR 16093 Department of Veterans Affairs Identity Management System (VAIDMS)-VA (3/26/2008) https://www.govinfo.gov/content/pkg/FR-2008-03-26/pdf/E8-6120.pdf
  - GSA/GOVT-7 / 80 FR 64416, HSPD-12 USAccess (11/23/2015) https://www.federalregister.gov/documents/2015/10/23/2015-26940/privacy-act-of-1974-notice-of-an-updated-system-of-records
- AUTHORITY FOR MAINTENANCE OF THE SYSTEM:
  - 5 U.S.C. 301;
  - Federal Information Security Management Act of 2002 (44 U.S.C. 3554)
  - E-Government Act of 2002 (Pub. L. 107-347, Sec. 203)
  - Paperwork Reduction Act of 1995 (44 U.S.C. 3501 et al.) and Government Paperwork Elimination Act (Pub. L. 105-277, 44 U.S.C. 3504 note)
  - Homeland Security Presidential Directive 12 (HSPD-12), Policy for a Common Identification Standard for Federal Employees and Contractors, August 27, 2004

I. If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval? If the system is using cloud technology, does the SORN for the system cover cloud usage or storage?

There are no current system changes that will result in modifications to the SORN; the system is not using cloud technology.

4. System Changes

J. Will the completion of this PIA will result in circumstances that require changes to business processes?

No

K. Will the completion of this PIA could potentially result in technology changes?

No

Section 1. Characterization of the Information

The following questions are intended to define the scope of the information requested and collected as well as the reasons for its collection as part of the program, IT system, or technology being developed.

1.1 What information is collected, used, disseminated, created, or maintained in the system?

Identify and list all Sensitive Personal Information (SPI) that is collected and stored in the system, including Individually Identifiable Information (III), Individually Identifiable Health Information (IIHI), Protected Health Information (PHI), and Privacy- Protected Information. For additional information on these information types and definitions, please see VA Directives and Handbooks in the 6500 series (https://vaww.va.gov/vapubs/). If the system creates information (for example, a score, analysis, or report), list the information the system is responsible for creating.

If a requesting system receives information from another system, such as a response to a background check, describe what information is returned to the requesting system.
This question is related to privacy control AP-1, Authority To Collect, and AP-2, Purpose Specification.

The information selected below must match the information provided in question 2.1 as well as the data elements columns in 4.1 and 5.1. It must also match the information provided in question 3.4 of the PTA.

Please check any information listed below that your system collects, uses, disseminates, creates, or maintains. If additional SPI is collected, used, disseminated, created, or maintained, please list those in the text box below:

- ☒ Name
- ☒ Social Security Number
- ☒ Date of Birth
- ☐ Mother's Maiden Name
- ☒ Personal Mailing Address
- ☒ Personal Phone Number(s)
- ☐ Personal Fax Number
- ☐ Personal Email Address
- ☐ Emergency Contact Information (Name, Phone Number, etc. of a different individual)
- ☐ Financial Information
- ☐ Health Insurance Beneficiary Numbers Account numbers
- ☐ Certificate/License numbers[1]
- ☐ Vehicle License Plate Number
- ☐ Internet Protocol (IP) Address Numbers
- ☐ Medications
- ☐ Medical Records
- ☒ Race/Ethnicity
- ☐ Tax Identification Number
- ☐ Medical Record Number
- ☒ Gender
- ☐ Integrated Control Number (ICN)
- ☐ Military History/Service Connection
- ☐ Next of Kin
- ☒ Other Data Elements (list below)

Other PII/PHI data elements:

[1] *Specify type of Certificate or License Number (e.g., Occupational, Education, Medical)

Country of birth, country of citizenship, biometrics, background investigation suitability decision, height, weight, eye color, hair color.

PII Mapping of Components (Servers/Database)

NextGen PIV maps to one VA internal component/database housing VA's Master Person Index. Analysis was completed to determine if any elements of that component collect PII. The type of PII collected by NextGen PIV and the reasons for the collection of the PII are in the table below.

Note: Due to the PIA being a public facing document, please do not include server names in the table. The first table of 3.9 in the PTA should be used to answer this question.

Internal Components Table

Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
VA Master Person Index	Yes	Yes	Name, Social Security Number, Date of Birth, Address, Phone Number, Country of Birth, Country of Citizenship, biometrics, background investigation suitability decision, height, weight, eye color, hair color, race and gender.	Identity Verification	TLS 2.1

1.2 What are the sources of the information in the system?

These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

1.2a List the individual, entity, or entities providing the specific information identified above. For example, is the information collected directly from the individual as part of an application for a benefit, or is it collected from other sources such as commercial data aggregators?

Initial information regarding a PIV applicant is collected by a credentialed agency sponsor either directly from the individual or from VA-approved forms completed by the individual as part of their onboarding. This information establishes an identity record for the individual and they subsequently complete an in-person "enrollment," during which, biographic and biometric information is collected.

1.2b Describe why information from sources other than the individual is required? For example, if a program's system is using data from a commercial aggregator of information or data taken from public Web sites, state the fact that this is where the information is coming from and then in question indicate why the system is using this source of data.

All information is collected either directly from the individual or from VA-approved forms completed by the individual as part of on-boarding in order to ensure accurate identity and VA affiliation/account information are included in PIV sponsorship and subsequent card issuance.

1.2c Does the system create information (for example, a score, analysis, or report), list the system as a source of information?

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.

1.3 How is the information collected?

These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

1.3a This question is directed at the means of collection from the sources listed in question 1.2. Information may be collected directly from an individual, received via electronic transmission from another system, or created by the system itself. Specifically, is information collected through technologies or other technologies used in the storage or transmission of information in identifiable form?

All information is collected either directly from the individual or from VA-approved forms completed by the individual as part of on-boarding. Integration with the VA Mast Person Index allows for transmission of identity, VA affiliation, and VA account information to NextGen PIV over a secure interface.

1.3b If the information is collected on a form and is subject to the Paperwork Reduction Act, what is the form's OMB control number and the agency form number?

Information for PIV sponsorship is not collected directly from OMB forms, though the PIV sponsor may rely Human Resources and Onboarding forms to complete required sponsorship fields.

1.4 How will the information be checked for accuracy? How often will it be checked?

These questions are related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.

1.4a Discuss whether and how often information stored in the system is checked for accuracy. Is information in the system checked against any other source of information (within or outside your organization) before the information is used to make decisions about an individual? For example, is there a computer matching agreement in place with another government agency? For systems that receive data from internal data sources or VA IT systems, describe the system checks to ensure that data corruption has not occurred during transmission.

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. Personal information such as Name and Date of Birth are reviewed and confirmed by the PIV applicant.

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.

1.4b Does the system check for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract?

The NextGen PIV system does not access a commercial information aggregator to check for accuracy.

1.5 What specific legal authorities, arrangements, and agreements defined the collection of information?

List the full legal authority for operating the system, specifically the authority to collect the information listed in question 1.1. Provide the authorities in a manner understandable to any potential reader, i.e., do not simply provide a legal citation; use statute names or regulations in addition to citations. Legal authorities include Federal laws, regulations, statutes, and Executive Orders. This question is related to privacy control AP-1, Authority to Collect

- GSA/GOVT-7 / 80 FR 64416, HSPD-12 USAccess (11/23/2015) https://www.federalregister.gov/documents/2015/10/23/2015-26940/privacy-act-of-1974-notice-of-an-updated-system-of-records
- 146VA005Q3/73 FR 16093 Department of Veterans Affairs Identity Management System (VAIDMS)-VA (3/26/2008) https://www.govinfo.gov/content/pkg/FR-2008-03-26/pdf/E8-6120.pdf
- Homeland Security Presidential Directive 12 (HSPD-12), C.F.R. 2014 Title 32, Vol.1, §161-4
- National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) 201-2: Personal Identity Verification (PIV) of Federal Employees and Contractors, §2.1-2.11
- 5 U.S.C. 301; Federal Information Security Management Act of 2002 (44 U.S.C. 3554)
- E-Government Act of 2002 (Pub. L. 107–347, Sec. 203)
- Paperwork Reduction Act of 1995 (44 U.S.C. 3501 et al.)
- Government Paperwork Elimination Act (Pub. L. 105–277, 44U.S.C. 3504 note)

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

Consider the specific data elements collected and discuss the potential privacy risks and what steps, if any are currently being taken to mitigate those identified risks. (*Work with your System ISSO to complete this section)*

Consider the following Fair Information Practice Principles (FIPPs) when assessing the risk to individual privacy:

Principle of Purpose Specification: Explain how the collection ties with the purpose of the underlying mission of the organization and its enabling authority.

Principle of Minimization: Is the information directly relevant and necessary to accomplish the specific purposes of the program?

Principle of Individual Participation: Does the program, to the extent possible and practical, collect information directly from the individual?

Principle of Data Quality and Integrity: Are there policies and procedures for VA to ensure that personally identifiable information is accurate, complete, and current?
This question is related to privacy control AR-1, Governance and Privacy Program, and AR-2, Privacy Impact and Risk Assessment.

Follow the format below when entering your risk assessment:

Privacy Risk: The privacy risk associated with this collection of PII is that VA staff members' PII could be inappropriately accessed, or that a VA staff member could be issued a credential with incorrect underlying PII.

Mitigation: To mitigate the risk of in inappropriate access to PII, USAccess employs the following:

- Privileged users of the USAccess system with access to PII are required to meet background investigation requirements (Tier 2 or higher), and successfully complete training course(s) associated with their assigned system role(s)
- Access to the system requires a valid PIV credential and certificate be present as part of 2-factor authentication processes
- Privileged users are required to annually read and digitally acknowledge/sign USAccess Rules of Behavior which outline proper handling of applicant PII
- The system is monitored to immediately identify anomalous activity, and completes and Annual Breach Response Exercise with the GSA Privacy Office

To safeguard against credentials being issued with incorrect underlying PII, the PIV credential issuance process includes:

- To find and open an applicant record, the system requires a matching combination of either: Last Name and Date of Birth, or Date of Birth and Social Security Number
- The PIV enrollment process includes stringent identity proofing, requiring the applicant present two forms of government-issued identification to validate PII against the system record prior to a credential being issued

Section 2. Uses of the Information

The following questions are intended to clearly delineate the use of information and the accuracy of the data being used.

2.1 Describe how the information in the system that will be used in support of the program's business purpose.

Identify and list each use (both internal and external to VA) of the information collected or maintained. This question is related to privacy control AP-2, Purpose Specification.

PII/PHI Data Element	Internal Use	External Use
Full Name:	Used to identify VA employee, contractor, or volunteer and complete	Not Used Externally

	requirements for PIV card adjudication and issuance	
Social Security Number	Used to identify VA employee, contractor, or volunteer and complete requirements for PIV card adjudication and issuance	Not Used Externally
Date of Birth	Used to identify VA employee, contractor, or volunteer and complete requirements for PIV card adjudication and issuance	Not Used Externally
Personal Mailing Address	Used to identify VA employee, contractor, or volunteer and complete requirements for PIV card adjudication and issuance	Not Used Externally
Personal Phone Number	Used to identify VA employee, contractor, or volunteer and complete requirements for PIV card adjudication and issuance	Not Used Externally
Race/Ethnicity	Used to identify VA employee, contractor, or volunteer and complete requirements for PIV card adjudication and issuance	Not Used Externally
Gender	Used to identify VA employee, contractor, or volunteer and complete requirements for PIV card adjudication and issuance	Not Used Externally
Country of Birth	Used to identify VA employee, contractor, or volunteer and complete requirements for PIV card adjudication and issuance	Not Used Externally
Country of Citizenship	Used to identify VA employee, contractor, or volunteer and complete requirements for PIV card adjudication and issuance	Not Used Externally
Biometrics	Used to identify VA employee, contractor, or volunteer and complete requirements for PIV card adjudication and issuance	Not Used Externally
Background Investigation Suitability Decision	Used to identify VA employee, contractor, or volunteer and complete	Not Used Externally

	requirements for PIV card adjudication and issuance	
Height	Used to identify VA employee, contractor, or volunteer and complete requirements for PIV card adjudication and issuance	Not Used Externally
Weight	Used to identify VA employee, contractor, or volunteer and complete requirements for PIV card adjudication and issuance	Not Used Externally
Eye Color	Used to identify VA employee, contractor, or volunteer and complete requirements for PIV card adjudication and issuance	Not Used Externally
Hair Color	Used to identify VA employee, contractor, or volunteer and complete requirements for PIV card adjudication and issuance	Not Used Externally

2.2 What types of tools are used to analyze data and what type of data may be produced?
These questions are related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information.

2.2a Many systems sift through large amounts of information in response to a user inquiry or programmed functions. Systems may help identify areas that were previously not obvious and need additional research by agents, analysts, or other employees. Some systems perform complex analytical tasks resulting in, among other types of data, matching, relational analysis, scoring, reporting, or pattern analysis. Describe any type of analysis the system conducts and the data that is created from the analysis?

NextGen PIV uses GSA's USAccess system and relies on a reciprocal ATO agreement. NextGen PIV has no control over the technical system. VA users connect to GSA USAccess using HTTPS.

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.

2.2b If the system creates or makes available new or previously unutilized information about an individual, explain what will be done with the newly derived information. Will it be placed in the individual's existing record? Will a new record be created? Will any action be taken against or for the individual identified because of the newly derived data? If a new record is created, will the newly created information be accessible to Government employees who make determinations about the individual? If so, explain fully under which circumstances and by whom that information will be used.

As a result of PIV sponsorship, the system creates an applicant sponsorship record withing NextGen PIV. This is information is used for the sole purpose of validating identity during the PIV enrollment process and issuing a PIV card. There will be no action taken against or for an applicant based on the information, and access is limited to only those Government staff who have completed training for the assigned role in the NextGen PIV system, for use in issuing and maintaining PIV cards.

2.3 How is the information in the system secured?

These questions are related to security and privacy controls SC-9, Transmission Confidentiality, and SC-28, Protection of Information at Rest.

2.3a What measures are in place to protect data in transit and at rest?

NextGen PIV uses GSA's USAccess system and relies on a reciprocal ATO agreement. NextGen PIV has no control over the technical system. VA users connect to GSA USAccess using HTTPS. 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 triennially.
- Application Role Holders complete training associated with their specific role(s) in the PIV issuance and maintenance processes.

2.3b If the system is collecting, processing, or retaining Social Security Numbers, are there additional protections in place to protect SSNs?

The system does collect and retain Social Security Numbers. NextGen PIV uses GSA's USAccess system and relies on a reciprocal ATO agreement. NextGen PIV has no control over the technical system. VA users connect to GSA USAccess using HTTPS. 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.

2.3c How is PII/PHI safeguarded in accordance with OMB Memorandum M-06-15?

NextGen PIV uses GSA's USAccess system and relies on a reciprocal ATO agreement. NextGen PIV has no control over the technical system. VA users connect to GSA USAccess using HTTPS. 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.

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information.

Describe any types of controls that may be in place to ensure that information is handled in accordance with the uses described above. Example: Describe if training for users of the project covers how to appropriately use information. Describe the disciplinary programs or system controls (i.e. denial of access) that are in place if an individual is inappropriately using the information.

Consider the following FIPPs below to assist in providing a response:

Principle of Transparency: Is the PIA and SORN, if applicable, clear about the uses of the information?

Principle of Use Limitation: Is the use of information contained in the system relevant to the mission of the project?
This question is related to privacy control AR-4, Privacy Monitoring and Auditing, AR-5, Privacy Awareness and Training, and SE-2, Privacy Incident response.

2.4a How is access to the PII determined?

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)

2.4b Are criteria, procedures, controls, and responsibilities regarding access documented?

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 GSA, 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).

2.4c Does access require manager approval?

All access requires approval by a designated Application or Agency Role Administrator. Role Administrators validate that proper role-based training is complete and that required background investigation level is satisfied prior to granting access.

2.4d Is access to the PII being monitored, tracked, or recorded?

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.

2.4e Who is responsible for assuring safeguards for the PII?

As the overall system owner, GSA is responsible for system safeguards for PII. NextGen PIV uses GSA's USAccess system and relies on a reciprocal ATO agreement.

Section 3. Retention of Information

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 What information is retained?

*Identify and list all information collected from question 1.1 that is **retained** by the system. This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal*

As described in System of Records Notice (SORN) GSA/GOVT-7 / 80 FR 64416, HSPD-12 USAccess (11/23/2015), 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: Name, Social Security Number, Date of Birth, Address, Phone Number, Country of Birth, Country of Citizenship, biometrics, background investigation suitability decision, height, weight, eye color, hair color, race and gender.

3.2 How long is information retained?

In some cases, VA may choose to retain files in active status and archive them after a certain period of time. State active file retention periods, as well as archived records, in number of years, for the information and record types. For example, financial data held within your system may have a different retention period than medical records or education records held within your system, please be sure to list each of these retention periods. ***The VA records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented.*** *If the system is using cloud technology, will it be following the NARA approved retention length and schedule? This question is related to privacy control DM-2, Data Retention and Disposal.*

Records relating to persons covered by this system are retained in accordance with General Records Schedule 5.6, Item 120. **Temporary.** Destroy 6 years after the end of an employee or contractor's tenure, but longer retention is authorized if required for business use. Unless retained for specific, ongoing security investigations, and in accordance with NARA, all the PIV collected data will be retained for a minimum of 6 years beyond the term of employment, unless otherwise directed. In accordance with HSPD–12, PIV Cards are deactivated within 18 hours from the notification time for cardholder separation, loss of card, or expiration. The information on PIV Cards is maintained in accordance with General Records Schedule 5.6, Item 121. PIV Cards are destroyed by shredding, within 90 days after deactivation.

Disposition of records will be according to VA OIT RCS 006-1 GRS 5.6-120 and VA OIT RCS 006-1, GRS 5.6-121.

3.3 Has the retention schedule been approved by the VA records office and the National Archives and Records Administration (NARA)?

An approved records schedule must be obtained for any IT system that allows the retrieval of a record via a personal identifier. The VA records officer will assist in providing a proposed schedule. The schedule must be formally offered to NARA for official approval. Once NARA approves the proposed schedule, the VA records officer will notify the system owner. Please work with the system Privacy Officer and VA Records Officer to answer these questions.
This question is related to privacy control DM-2, Data Retention and Disposal.

3.3a Are all records stored within the system of record indicated on an approved disposition authority?

All records stored within this system are in accordance with the General Record Schedule.

3.3b Please indicate each records retention schedule, series, and disposition authority?

Disposition of records will be according to the General Record Schedule, section 5.6 items 120 and 121, which can be found at the following URL:
https://www.archives.gov/files/records-mgmt/grs/grs05-6.pdf

3.4 What are the procedures for the elimination or transfer of SPI?

Explain how records are destroyed, eliminated or transferred to NARA at the end of their mandatory retention period. Please give the details of the process. For example, are paper records shredded

on site, or by a shredding company and accompanied by a certificate of destruction, etc.? This question is related to privacy control DM-2, Data Retention and Disposal.

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.

Disposition of records will be according to GRS 5.6-120 and GRS 5.6-121. USAccess sponsorship and enrollment records which have not held an Active employment status in the system for 6 years or longer will be destroyed through routine system-automated processes managed by GSA.

In accordance with HSPD–12, physical PIV Cards are deactivated within 18 hours from the notification time for cardholder separation, loss of card, or expiration. The information on PIV Cards is maintained in accordance with General Records Schedule 5.6, Item 121. PIV Cards are destroyed by shredding on-site, within 90 days after deactivation.

3.5 Does the system, where feasible, use techniques to minimize the risk to privacy by using PII for research, testing, or training?

Organizations often use PII for testing new applications or information systems prior to deployment. Organizations also use PII for research purposes and for training. These uses of PII increase the risks associated with the unauthorized disclosure or misuse of the information. Please explain what controls have been implemented to protect PII used for testing, training and research. This question is related to privacy control DM-3, Minimization of PII Used in Testing, Training and Research.

NextGen PIV uses GSA's USAccess system and relies on a reciprocal ATO agreement. NextGen PIV has no control over the technical system. VA users connect to GSA USAccess using HTTPS. The USAccess program and system active data is not used for research, testing, or training.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

Discuss the risks associated with the length of time data is retained and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

While we understand that establishing retention periods for records is a formal process, there are policy considerations behind how long a project keeps information. The longer a project retains information, the longer it needs to secure the information and assure its accuracy and integrity. The proposed schedule should match the requirements of the Privacy Act to keep the minimum amount of PII for the minimum amount of time, while meeting the Federal Records Act. The schedule should align with the stated purpose and mission of the system.

Consider the following FIPPs below to assist in providing a response:

Principle of Minimization: Does the project retain only the information necessary for its purpose? Is the PII retained only for as long as necessary and relevant to fulfill the specified purposes?

Principle of Data Quality and Integrity: Has the PIA described policies and procedures for how PII that is no longer relevant and necessary is purged?

This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal.

Follow the format below:

Privacy Risk: NextGen PIV uses GSA's USAccess system and relies on a reciprocal ATO agreement. NextGen PIV has no control over data or systems. VA users connect to GSA USAccess using HTTPS.

The privacy risk associated with the retention of data for the required amount of time involves unauthorized access through network intrusion or due to possible negligence be it willful or inadvertent.

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.

Mitigation: 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 4. Internal Sharing/Receiving/Transmitting and Disclosure

The following questions are intended to define the scope of information sharing/receiving/transmitting within VA.

4.1 With which internal organizations is information shared/received/transmitted? What information is shared/received/transmitted, and for what purpose? How is the information transmitted?

NOTE: Question 3.9 (second table) on Privacy Threshold Analysis should be used to answer this question.

Identify and list the names of any program offices, contractor-supported IT systems, and any other organization or IT system within VA with which information is shared.

State the purpose for the internal sharing. If you have specific authority to share the information, provide a citation to the authority.

For each interface with a system outside your program office, state what specific data elements (PII/PHI) are shared with the specific program office, contractor-supported IT system, and any other organization or IT system within VA.

Describe how the information is transmitted. For example, is the information transmitted electronically, by paper, or by some other means? Is the information shared in bulk, on a case-by-case basis, or does the sharing partner have direct access to the information?
This question is related to privacy controls AP-2, Purpose Specification, AR-3, Privacy Requirements for Contractors and Service Providers, AR-8, Accounting of Disclosures, TR-1, Privacy Notice, and UL-1, Internal Use.

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system***	***Describe the method of transmittal***
VA Identity and Access Management	Identity Verification	Name, Social Security Number, Date of Birth, Address, Phone Number, Country of Birth, Country of Citizenship, biometrics, background investigation suitability decision, height, weight, eye color, hair color, race and gender.	System Infrastructure Provider (SIP) interface using HTTPS

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

Discuss the privacy risks associated with the sharing of information within the Department and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

This question is related to privacy control UL-1, Internal Use.

Follow the format below:

Privacy Risk: NextGen PIV uses GSA's USAccess system and relies on a reciprocal ATO agreement. NextGen PIV has no control over the technical system. VA users connect to GSA USAccess using HTTPS. The privacy risk associated with internal sharing and disclosure of information can be due to possible negligence be it willful or inadvertent.

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.

Mitigation: Personnel accessing the GSA USAccess system must read and acknowledge their receipt and acceptance of the VA National Rules of Behavior (ROB) or VA Contractor's ROB prior to gaining access to any VA information system or sensitive information. The rules are included as part of the security awareness training which all personnel must complete via the VA's Talent Management System (TMS). The rules state the terms and conditions that apply to personnel who are provided access to, or use of, information, including VA sensitive information, or VA information systems, such as no expectation of privacy, and acceptance of monitoring of actions while accessing the system. After the user's initial acceptance of the Rules, the user must re-affirm their acceptance annually as part of the security awareness training.

Acceptance obtained through electronic acknowledgment is tracked through the TMS system. All VA employees must complete annual Privacy and Security training. VEMS users agree to comply with all terms and conditions of the VA National ROB by signing a certificate of training at the end of the training session.

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. Role Holders are required to take training for the role they have been assigned and provide certificate as proof of completion. 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.

Section 5. External Sharing/Receiving and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to VA, which includes Federal, State, and local governments, and the private sector.

5.1 With which external organizations (outside VA) is information shared/received? What information is shared/received, and for what purpose? How is the information transmitted and what measures are taken to ensure it is secure?

Is the sharing of information outside the agency compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If not, please describe under what legal mechanism the IT system is allowed to share the information in identifiable form or personally identifiable information outside of VA.

NOTE: Question 3.10 on Privacy Threshold Analysis should be used to answer this question.

Identify and list the names of any Federal, State, or local government agency or private sector organization with which information is shared.

For each interface with a system outside VA, state what specific data elements (PII/PHI) are shared with each specific partner.

What legal mechanisms, authoritative agreements, documentation, or policies are in place detailing the extent of the sharing and the duties of each party? For example, is the sharing of data compatible with your SORN? Then list the SORN and the applicable routine use from the SORN. Is there a Memorandum of Understanding (MOU), Computer Matching Agreement (CMA), or law that mandates the sharing of this information?

Describe how the information is transmitted to entities external to VA and what security measures have been taken to protect it during transmission.
This question is related to privacy control UL-2, Information Sharing with Third Parties

Data Shared with External Organizations

List External Program Office or IT System information is shared/received with	***List the purpose of information being shared / received / transmitted with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program or IT system***	***List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)***	***List the method of transmission and the measures in place to secure data***
General Services	Identity and Credential	Name, Social Security Number, Date of Birth, Address, Phone Number,	VAIDMS SORN	System Infrastructure Provider

Administration (GSA)	Management/GSA USAccess	Country of Birth, Country of Citizenship, biometrics, background investigation suitability decision, height, weight, eye color, hair color, race and gender.	146VA005Q3 GSA SORN 80 FR 64416	(SIP) interface using HTTPS

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

Discuss the privacy risks associated with the sharing of information outside the Department and what steps, if any, are currently being taken to mitigate those identified risks.

If no External Sharing listed on the table above, ***(State there is no external sharing in both the risk and mitigation fields).***

Discuss whether access controls have been implemented and whether audit logs are regularly reviewed to ensure appropriate sharing outside of the Department. For example, is there a Memorandum of Understanding (MOU), contract, or agreement in place with outside agencies or foreign governments.
Discuss how the sharing of information outside of the Department is compatible with the stated purpose and use of the original collection.
This question is related to privacy control AR-2, Privacy Impact and Risk Assessment, AR-3, Privacy Requirements for Contractors and Service Providers, and AR-4, Privacy Monitoring and Auditing

Follow the format below:

Privacy Risk: The privacy risks associated with the external sharing and disclosure of information outside the VA are inadvertent access and data breach.

Mitigation: 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.

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.

Section 6. Notice

The following questions are directed at providing notice to the individual of the scope of information collected, the right to consent to uses of the information, and the right to decline to provide information.

6.1 Was notice provided to the individual before collection of the information? If yes, please provide a copy of the notice as an Appendix-A 6.1 on the last page of the document. Also provide notice given to individuals by the source system (A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register.) If notice was not provided, why not?

These questions are related to privacy control TR-1, Privacy Notice, and TR-2, System of Records Notices and Privacy Act Statements, and TR-3, Dissemination of Privacy Program Information.

6.1a This question is directed at the notice provided before collection of the information. This refers to whether the person is aware that his or her information is going to be collected. A notice may include a posted privacy policy, a Privacy Act statement on forms, or a SORN published in the Federal Register, Notice of Privacy Practice provided to individuals for VHA systems. If notice was provided in the Federal Register, provide the citation.

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.
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:

The SORNs for the system are GSA's USAccess SORN and VAIDMS SORN 146VA005Q3

6.1b If notice was not provided, explain why. If it was provided, attach a copy of the current notice.

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.

6.1c Describe how the notice provided for the collection of information is adequate to inform those affected by the system that their information has been collected and is being used appropriately. Provide information on any notice provided on forms or on Web sites associated with the collection.

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.

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:

6.2 Do individuals have the opportunity and right to decline to provide information? If so, is a penalty or denial of service attached?

This question is directed at whether the person from or about whom information is collected can decline to provide the information and if so, whether a penalty or denial of service is attached. This question is related to privacy control IP-1, Consent, IP-2, Individual Access, and IP-3, Redress.

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.

6.3 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

This question is directed at whether an individual may provide consent for specific uses, or the consent is given to cover all uses (current or potential) of his or her information. If specific consent is required, how would the individual consent to each use? This question is related to privacy control IP-1, Consent.

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.

6.4 <u>PRIVACY IMPACT ASSESSMENT: Notice</u>

Describe the potential risks associated with potentially insufficient notice and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

Consider the following FIPPs below to assist in providing a response:

Principle of Transparency: Has sufficient notice been provided to the individual?

Principle of Use Limitation: Is the information used only for the purpose for which notice was provided either directly to the individual or through a public notice? What procedures are in place to ensure that information is used only for the purpose articulated in the notice?
This question is related to privacy control TR-1, Privacy Notice, AR-2, Privacy Impact and Risk Assessment, and UL-1, Internal Use.
Follow the format below:

Privacy Risk: The potential risks associated with insufficient notice are user may not have a USAccess card issued, have errors on their USAccess card, and may not be able to access systems required for job duties.

Mitigation: 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)

Section 7. Access, Redress, and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about him or her.

7.1 What are the procedures that allow individuals to gain access to their information?
These questions are related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.

7.1a Cite any procedures or regulations your program has in place that allow access to information. These procedures, at a minimum, should include the agency's FOIA/Privacy Act practices, but may also include additional access provisions. ***For example, if your program has a customer satisfaction unit, that information, along with phone and email contact information, should be listed in this section in addition to the agency's procedures. See 5 CFR 294 and the VA FOIA Web page at http://www.foia.va.gov/ to obtain information about FOIA points of contact and information about agency FOIA processes.***

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 Managed Service Office (MSO).

7.1b If the system is exempt from the access provisions of the Privacy Act, please explain the basis for the exemption or cite the source where this explanation may be found, for example, a Final Rule published in the Code of Federal Regulations (CFR)?

The system is not exempt from Privacy Act provisions.

7.1c If the system is not a Privacy Act system, please explain what procedures and regulations are in place that covers an individual gaining access to his or her information?

The system is a Privacy Act system.

7.2 What are the procedures for correcting inaccurate or erroneous information?

Describe the procedures and provide contact information for the appropriate person to whom such issues should be addressed? If the correction procedures are the same as those given in question 7.1, state as much. This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

A USAccess cardholder generally does not have the ability to directly access or modify information on themselves on a routine basis. If a cardholder 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).

7.3 How are individuals notified of the procedures for correcting their information?

How are individuals made aware of the procedures for correcting his or her information? This may be through notice at collection or other similar means. This question is meant to address the risk that even if procedures exist to correct information, if an individual is not made fully aware of the existence of those procedures, then the benefits of the procedures are significantly weakened. This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

GSA provides individuals the ability to access their PII and to correct or amend it if it is inaccurate. Individuals are requested verbally to verify information while application for USAccess card is being submitted. The information in USAccess is cross referenced with VA IAM to verify identity. If GSA exempts a system or program from access, amendment and other provisions of the Privacy Act, it notifies the public of that exemption.

7.4 If no formal redress is provided, what alternatives are available to the individual?

Redress is the process by which an individual gains access to his or her records and seeks corrections or amendments to those records. Redress may be provided through the Privacy Act and Freedom of Information Act (FOIA), and also by other processes specific to a program, system, or

group of systems. ***Example: Some projects allow users to directly access and correct/update their information online. This helps ensures data accuracy.***
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

A USAccess cardholder generally does not have the ability to directly access or modify information on themselves. If a cardholder 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).

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

Discuss what risks there currently are related to the Department's access, redress, and correction policies and procedures for this system and what, if any, steps have been taken to mitigate those risks. ***For example, if a project does not allow individual access, the risk of inaccurate data needs to be discussed in light of the purpose of the project. For example, providing access to ongoing law enforcement activities could negatively impact the program's effectiveness because the individuals involved might change their behavior.*** *(Work with your System ISSO to complete all Privacy Risk questions inside the document this section).*

Consider the following FIPPs below to assist in providing a response:
Principle of Individual Participation: Is the individual provided with the ability to find out whether a project maintains a record relating to him?

Principle of Individual Participation: If access and/or correction is denied, then is the individual provided notice as to why the denial was made and how to challenge such a denial?

Principle of Individual Participation: Is there a mechanism by which an individual is able to prevent information about him obtained for one purpose from being used for other purposes without his knowledge?
This question is related to privacy control IP-3, Redress.

Follow the format below:

Privacy Risk: Individuals are required to verify the information they have provided is correct. If the information is incorrect, the individual specifies the incorrect information and provides the correct information. The information is then verified as correct prior to a PIV Badge being printed. If information is not correct, the badge will not print. The system uses various data points and compares to verify the individual is who they say they are. If the individual decides to not provide identity information, the individual will not be issued a card or be able to access sites and resources required for job duties and will not be able to maintain employment with the VA.

Access to the USAccess system is limited to role holders. Role holders work with individuals to gather personal information to issue the USAccess cards. Individuals will verify the information prior to USAccess card issuance. The information stored in USAccess will not be used for other purposes.

Mitigation: 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 can 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. Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

8.1 What procedures are in place to determine which users may access the system, and are they documented?

These questions are related to privacy control AR-7, Privacy-Enhanced System Design and Development.

8.1a Describe the process by which an individual receives access to the system?

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.

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).

8.1b Identify users from other agencies who may have access to the system and under what roles these individuals have access to the system. Who establishes the criteria for what PII can be shared?

Other agency users with access to VA data are limited to only those approved and credentialed GSA staff assigned the Application Administrator role. Access for administrative users is managed by GSA, 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).

8.1c Describe the different roles in general terms that have been created to provide access to the system? For example, certain users may have "read-only" access while others may be permitted to make certain amendments or changes to the information.

Application Administrator: GSA approved and credentialed technical and program staff to manage the overall system for all customers
Agency Site Manager: Manages all VA site functions, such as appointment availability and establishment of new credentialing sites in the system. No access to PII.
Local Site Manager: Manages single site functions, such as appointment availability. No access to PII.
Agency Role Administrator: Responsible for properly vetting individuals seeking access to the system, ensuring proper background investigations and training have been completed. Once vetting is complete, the requested system roles can be granted.
Agency Security Officer: Responsible for overall maintenance of applicant records and resolution of data quality issues.
Sponsor: Creates new applicant records for staff requiring a PIV issuance based on PII data collected from the applicant.
Adjudicator: Ensures that proper adjudicative documentation (special agreement check (SAC), background investigation) is in place for PIV applicants prior to approving PIV issuance.
Registrar: Conducts in-person identity proofing with PIV applicants and captures identification documentation and biometrics in the system as part of enrollment for PIV issuance.
Activator: Activates printed PIV cards for applicants. No access to PII.
Print Operator: Locally prints PIV cards for applicants who have completed enrollment and have been favorably adjudicated. No access to PII.
Report Viewer: Read-only access to run reports from the USAccess portal. PII access is limited to only DOB; SSN is not included in any reports.
Credential Inventory Tool Operator: Manages PIV issuing site inventory of cardstock and printing consumables; orders additional stock when necessary. No access to PII.

8.2 Will VA contractors have access to the system and the PII? If yes, what involvement will contractors have with the design and maintenance of the system? Has a contractor confidentiality agreement, Business Associate Agreement (BAA), or a Non-Disclosure Agreement (NDA) been developed for contractors who work on the system?

If so, how frequently are contracts reviewed and by whom? Describe the necessity of the access provided to contractors to the system and whether clearance is required. If Privacy Roles and Responsibilities have been established to restrict certain users to different access levels, please describe the roles and associated access levels. Explain the need for VA contractors to have access to the PII. This question is related to privacy control AR-3, Privacy Requirements for Contractors, and Service Providers.

VA contractors do have access to the system and PII in cases where an appropriate background investigation is completed favorably, an associated NDA is signed and archived, and required training is completed. However, contractors are not permitted to serve in Sponsor or

Adjudicator roles in USAccess. 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 GSA, 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). All contractors that have access to the system have signed Non-Disclosure Agreements (NDA).

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

VA offers privacy and security training. Each program or system may offer training specific to the program or system that touches on information handling procedures and sensitivity of information. Please describe how individuals who have access to PII are trained to handle it appropriately. This question is related to privacy control AR-5, Privacy Awareness and Training.

All VA staff are required to complete the following training courses prior to being granted access to the VA network and/or any VA systems, with annual refreshers also required to maintain access:

- VA 10176: Privacy and Info Security Awareness and Rules of Behavior
- VA 10203: Privacy and HIPAA Training
- VA 3812493: Annual Government Ethics Role-based Training, which includes, but is not limited to and based on the role of the user.
    - VA 1016925: Information Assurance for Software Developers IT Software Developers
    - VA 3195: Information Security for CIOs Executives, Senior Managers, CIOs and CFOs
    - VA 1357084: Information Security Role-Based Training for Data Managers
    - VA 64899: Information Security Role-Based Training for IT Project Managers
    - VA 3197: Information Security Role-Based Training for IT Specialists

- VA 1357083: Information Security Role-Based Training for Network Administrators
- VA 1357076: Information Security Role-Based Training for System Administrators
- VA 1337064: Information Security for Facilities Engineers
- VA 1016923: Information Security Role-Based Training for Human Resources Professionals
- VA 3193: Information Security for CIOs

Additionally, all users requesting access to the USAccess system must complete the GSA USAccess role-based training course associated with the role they are questing, and provide proof of completion in the form of a training certificate. Available USAccess roles are outlined in section 8.1 of this PIA.

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, HIPAA, 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. Role holders are required to upload certificates to SharePoint prior to being granted the assigned roles.

8.4 Has Authorization and Accreditation (A&A) been completed for the system?

8.4a If Yes, provide:

1. *The Security Plan Status:* Approved
2. *The System Security Plan Status Date:* December 22, 2023
3. *The Authorization Status:* Authorization to Operate (ATO)
4. *The Authorization Date:* May 4, 2024
5. *The Authorization Termination Date:* May 4, 2027
6. *The Risk Review Completion Date:* April 10, 2024
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* Moderate

Please note that all systems containing SPI are categorized at a minimum level of "moderate" under Federal Information Processing Standards Publication 199.

NextGen PIV manages a VA Authority to Operate based on reciprocating GSA's ATO for USAccess. VA information security subject matter experts review GSA's ATO documentation on an annual basis prior to granting the VA ATO.

GSA has maintained a System Security Plan (SSP) and a FISMA ATO for the USAccess system since the service was rolled out within the federal government. The current ATO was issued on March 15, 2024.

8.4b If No or In Process, provide your ***Initial Operating Capability (IOC) date.***

ATO is in place for this system.

Section 9 – Technology Usage

The following questions are used to identify the technologies being used by the IT system or project.

9.1 Does the system use cloud technology? If so, what cloud model is being utilized?

If so, Does the system have a FedRAMP provisional or agency authorization? If the system does use cloud technology, but does not have FedRAMP authorization, explain how the Cloud Service Provider (CSP) solution was assessed and what FedRAMP documents and processes were used for the assessment in order to comply with VA Handbook 6517. Types of cloud models include: Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Commercial off the Shelf (COTS), Desktop as a Service (DaaS), Mobile Backend as a Service (MBaaS), Information Technology Management as a Service (ITMaaS). This question is related to privacy control UL-1, Information Sharing with Third Parties.

***Note: For systems utilizing the VA Enterprise Cloud (VAEC), no further responses are required after 9.1**. (Refer to question 3.3.1 of the PTA)*

GSA USAccess does not use a cloud service provider.

9.2 Does the contract with the Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII? (Provide contract number and supporting information about PII/PHI from the contract). (*Refer to question 3.3.2 of the PTA) This question is related to privacy control AR-3, Privacy Requirements for Contractors, and Service Providers.*

GSA USAccess does not use a cloud service provider.

USAccess uses an on premise solution. Locations are:

- GSA USAccess Primary Data Center:
  250 Burlington Drive
  Clarksville, VA 23927-3201
- GSA USAccess Recovery Data Center:
  311 Rockrimmon Blvd. South
  Colorado Springs, CO 80919

9.3 Will the CSP collect any ancillary data and if so, who has ownership over the ancillary data?

Per NIST 800-144, cloud providers hold significant details about the accounts of cloud consumers that could be compromised and used in subsequent attacks. Ancillary data also involves information the cloud provider collects or produces about customer-related activity in the cloud. It includes data collected to meter and charge for consumption of resources, logs and audit trails, and other such metadata that is generated and accumulated within the cloud environment.

This question is related to privacy control DI-1, Data Quality.

GSA USAccess does not use a cloud service provider.

9.4 NIST 800-144 states, "Organizations are ultimately accountable for the security and privacy of data held by a cloud provider on their behalf." Is this principle described in contracts with customers? Why or why not?

What are the roles and responsibilities involved between the organization and cloud provider, particularly with respect to managing risks and ensuring organizational requirements are met? This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.

GSA USAccess does not use a cloud service provider.

9.5 If the system is utilizing Robotics Process Automation (RPA), please describe the role of the bots.

Robotic Process Automation is the use of software scripts to perform tasks as an automated process that executes in parallel with or in place of human input. For example, will the automation move or touch PII/PHI information. RPA may also be referred to as "Bots" or Artificial Intelligence (AI).

GSA's USAccess system does not utilize Robotics Process Automation (RPA).

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

ID	Privacy Controls
AP	**Authority and Purpose**
AP-1	Authority to Collect
AP-2	Purpose Specification
AR	**Accountability, Audit, and Risk Management**
AR-1	Governance and Privacy Program
AR-2	Privacy Impact and Risk Assessment
AR-3	Privacy Requirements for Contractors and Service Providers
AR-4	Privacy Monitoring and Auditing
AR-5	Privacy Awareness and Training
AR-7	Privacy-Enhanced System Design and Development
AR-8	Accounting of Disclosures

ID	Privacy Controls
DI	**Data Quality and Integrity**
DI-1	Data Quality
DI-2	Data Integrity and Data Integrity Board
DM	**Data Minimization and Retention**
DM-1	Minimization of Personally Identifiable Information
DM-2	Data Retention and Disposal
DM-3	Minimization of PII Used in Testing, Training, and Research
IP	**Individual Participation and Redress**
IP-1	Consent
IP-2	Individual Access
IP-3	Redress
IP-4	Complaint Management
SE	**Security**
SE-1	Inventory of Personally Identifiable Information
SE-2	Privacy Incident Response
TR	**Transparency**
TR-1	Privacy Notice
TR-2	System of Records Notices and Privacy Act Statements
TR-3	Dissemination of Privacy Program Information
UL	**Use Limitation**
UL-1	Internal Use
UL-2	Information Sharing with Third Parties

Signature of Responsible Officials

The individuals below attest that the information they provided in this Privacy Impact Assessment is true and accurate.

JULIE DRAKE Digitally signed by JULIE DRAKE
Date: 2024.08.12 13:37:21 -06'00'

Privacy Officer, Julie Drake

ANITA FEIERTAG Digitally signed by ANITA FEIERTAG
Date: 2024.08.12 15:47:33 -04'00'

Information System Security Officer, Anita Feiertag

REED MEYER Digitally signed by REED MEYER
Date: 2024.08.12 15:28:01 -04'00'

Information System Owner, Reed Meyer

Please provide a link to the notice or verbiage referred to in Section 6 (a notice may include a posted privacy policy; a Privacy Act notice on forms; screen shot of a website collection privacy notice).

Link to GSA's USAccess PIA

Link to GSA's USAccess SORN

Link to: VAIDMS SORN 146VA005Q3

Link to: VA OPRM current SORNs

HELPFUL LINKS:

General Records Schedule
https://www.archives.gov/records-mgmt/grs.html

National Archives (Federal Records Management):
https://www.archives.gov/records-mgmt/grs

VA Publications:
https://www.va.gov/vapubs/

VA Privacy Service Privacy Hub:
https://dvagov.sharepoint.com/sites/OITPrivacyHub

Notice of Privacy Practice (NOPP):
VHA Notice of Privacy Practices
VHA Handbook 1605.04: Notice of Privacy Practices