Privacy Impact Assessment for the VA IT System called:

VACO – PIV Assessing (PIV)

VACO

Office of Information Technology (OIT)

Date PIA submitted for review:

02/02/2023

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Julie Drake	Julie.drake@va.gov	202-632-8431
Information System Security Officer	Derek Sterns	Derek.sterns@va.gov	804-585-6015
Information System Owner	Jason Miller	Jason.miller5@va.gov	630-421-2133

Abstract

The abstract provides the simplest explanation for "what does the system do?" and will be published online to accompany the PIA link.

VACO – Personal Identity Verification (PIV) Assessing provides a secure web interface for users to access the PIV system so that they can securely manage the processing of PIV and Non-PIV card applications, to include electronic data submission and biometrics capture. VACO-PIV Assessing processes personal identity information to generate a credential used for both logical and physical access. This information includes, but is not limited to, user identification, user role information, access information, passwords, PIV card data, digital certificates, and unlock codes.

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. The IT system name and the name of the program office that owns the IT system.

VACO - PIV Assessing is owned and operated by the VA Office of Information and Technology (OI&T)

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

In March 2009, the Department of Veterans Affairs (VA) began efforts to establish a system of PIV cards which would comply with and fulfill the objectives of HSPD-12. The Office of Information and Technology (OIT) under the authority of the VA is responsible for the analysis, design, implementation, operations and maintenance, service desk functions, field site deployment, full software development life cycle, and hardware/software procurement as it relates to the VA PIV program. VACO-PIV Assessing is a fully functional and FIPS 201-compliant system used by all VA organizations to issue and manage PIV and non-PIV cards through a web interface.

C. Indicate the ownership or control of the IT system or project.

VA OI&T

2. Information Collection and Sharing

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

The VA has approximately from 680.000 to 720.000 records.

E. A general description of the information in the IT system and the purpose for collecting this information.

VACO-PIV Assessing embraces a modular architecture based on the integration of enterprise class COTS products. This architectural approach allows the utilization of the best solution for each system function, while keeping the system highly customizable and scalable. The modular build enables individual elements of VACO-PIV Assessing to be replaced with minimal reintegration efforts, almost in a plug and play model. This model permits concentration on definition of VACO-PIV Assessing services (aka sub-systems) in terms of data models and information models that are meaningful to VA business units and facilitates integration to a well-defined VA Enterprise Architecture and enterprise solutions. VACO-PIV Assessing services (aka sub-systems) include

• Identity Management and Provisioning – Provides the services that manage the lifecycle of identity and VA card application records.

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

VACO-PIV Assessing shares an interconnection with Verizon Business. The Verizon Business Shared Service System is an authorized Shared Service Provider (SSP) established under the Federal Identity Credentialing Committee (FICC) and the Federal PKI Policy Authority. The Verizon Business Shared Service System provides the PKI services required by FIPS 201 and supports

VACO-PIV Assessing's requirements to issue and manage PKI certificates. All data transferred to Verizon Business is restricted using the principal of least privilege, more commonly referred to as "need-to-know." There is no personally identifiable information (PII) as defined by NIST SP 800-112 sent to the SSP.

G. Whether 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.

VACO-PIV Assessing is identified as a Major Application (MA) that is hosted in approved and secure VA Data Centers located in Hines, IL and Martinsburg, WV. VACO-PIV Assessing does not utilize cloud technology. Currently, VACO-PIV Assessing contains over 1.4 million records consisting of data received from US military veterans, VA employees, and VA contractors. The magnitude of harm and the damage to reputations that would be caused by a malicious or unintentional disclosure of PII is extreme. The data center buildings are occupied by the Department of Veterans Affairs' employees and contractors and are not open to the public.

3. Legal Authority and SORN

H. A citation of the legal authority to operate the IT system.

145 AUTHORITIES FOR MAINTENANCE OF THE SYSTEM: Executive Orders 9397, 10450, 10865,12333,
and 12356; 5 U.S.C 3301 and 9101; 42 U.S.C 2165 and 2201; 50 U.S.C 781 to 887; 5 C.F.R 5, 732, and 736; and Homeland Security Presidential Directive 12.

SORN:
145VA005Q3; "Department of Veterans Affairs Personnel Security File System (VAPSFS)-VA" (https://www.oprm.va.gov/privacy/systems_of_records.aspx).

https://www.govinfo.gov/content/pkg/FR-2022-07-01/pdf/2022-14118.pdf

103 AUTHORITIES FOR MAINTENANCE OF THE SYSTEM: 38 U.S.C. 501; 38 U.S.C. 901–905. 103VA07B; "Police and Security Records-ID-VA

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?

The SORN does not need to be modified or changed

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

No, it doesn't change the business process.

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

At this time, we do not anticipate that completion of this PIA will result in the need to make changes to any business processes or technology for the VA or its contractors.

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.

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*
☐ 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 forms of identification are Driver's License, Passport numbers, Biometrics - Fingerprints and photo ID

PII Mapping of Components (Servers/Database)

VACO – PIV Assessing consists of two key components. Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by VACO – PIV Assessing 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 the server names in the table. The first table of 3.9 in the PTA should be used to answer this question.

Internal Database Connections

Database Name of the information system collecting/storing PII	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
SQL Server	Yes	Yes	Driver's License, Biometric	Required for issue of PIV card	Physical: PIV Card to Access Datacenters Logical: Encrypted with 140-2, AES-256 cryptographic keys.
Oracle	Yes	Yes	Driver's License, Biometric	Required for issue of PIV card	Physical: PIV Card to Access Datacenters Logical: Encrypted with 140-2, AES-256 cryptographic keys.

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?

All information is collected directly from the veteran, the VA employee, the VA contractor, or the VA trainee.

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.

The information is collected from the veteran, the VA employee, or the VA contractor using Form 0711 OMB No. 2900-0673. This form is subject to the Paperwork Reduction Act. The information is processed through the enrollment portal, and it can only be accessed by certified PIV officials.
A copy of this form is located at
http://www.va.gov/OPTOMETRY/docs/vaform0711reqforidverificationcard.pdf.

1.2c If the system creates information (for example, a score, analysis, or report), list the system as a source of information.

No, this System does not create information

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?
This System doesn't receive information electronically from other IT Systems This System receives information directly from individuals.

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

The information is collected from the veteran, the VA employee, or the VA contractor using Form 0711 of OMB, Control No.2900-0673. This form is subject to the Paperwork Reduction Act. The information is processed through the enrollment portal, and it can only be accessed by certified PIV officials.
A copy of this form is located at:
http://www.va.gov/OPTOMETRY/docs/vaform0711reqforidverificationcard.pdf.

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.

Data is verified for accuracy by the applicant who is the source of the information and by an official system data registrar with the applicant's presentation of two forms of government-issued photo ID. All data that is required for the issuance of a PIV card is verified in this check. The system itself is a communication, workflow, and document repository, and provides no checks for accuracy or completeness.
The information provided by the applicant is not checked by the system against any other source of information within or outside the organization. There is no computer matching agreement in place with another government agency.

1.4b If the system checks for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract.

No, This System doesn't use a commercial aggregator.

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

145 AUTHORITIES FOR MAINTENANCE OF THE SYSTEM: Executive Orders 9397, 10450, 10865,12333, and 12356; 5 U.S.C 3301 and 9101; 42 U.S.C 2165 and 2201; 50 U.S.C 781 to 887; 5 C.F.R 5, 732, and 736; and Homeland Security Presidential Directive 12.

103 AUTHORITIES FOR MAINTENANCE OF THE SYSTEM: 38 U.S.C. 501; 38 U.S.C. 901–905.

1.6 <u>PRIVACY IMPACT ASSESSMENT: Characterization of the information</u>

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: If the data collected to issue a PIV card were not accurate, VA employees will not access the network or the facility.

Mitigation: VACO-PIV Assessing verifies the information from the employees using Active Directory, or through a background investigation.

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 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.

• Full Name Used to identify individual
• SSN Used to complete background check purposes
• Date of Birth Used to verify employee/contractor identity
• Mailing Address Used to communicate in writing with applicant when necessary
• Zip Code Used for mailing purpose
• Phone Number Used to contact applicant when necessary
• Email Used as alternate communication with applicant if necessary
• Mother's Maiden Name Used to verify employee/contractor identity
• Emergency Contact Used in case of emergency for contact information
• Race Used as necessary to plan for equal employment opportunity
• Passport Number Used to verify applicant identity
• Driver's License Used to verify applicant identity
• Taxpayers Identification Number Used to verify applicant's identity

• Fingerprints Used for background investigation
• Photographic image Used to the physical identify employee/contractor

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.

Correspondence is tracked in the system and reports are generated as needed. The system has the capability to differentiate the latest VA Form 0711 in the system by document type. These document types are established at the time the record is established in the system and assignments are made. If the system creates or makes available new or previously unutilized information about an individual, a new record will be created. There will not be any action taken against or for the individual identified because of the newly derived data. Also, only individuals who have been appointed, trained, and certified as PIV Officials (PCI Managers, Sponsors, Registrars, or Issuers) may access the VA PIV Enrollment Portal.
The facility PCI Manager is the appropriate point of contact for all information related to certification of system officials and access to the VA PIV Enrollment Portal. A PIV card is required to gain access to the VA PIV Enrollment Portal. There is no analysis conducted by VACO – PIV Assessing.

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.

If the system creates or makes available new or previously unutilized information about an individual, a new record will be created. There will not be any action taken against or for the individual identified because of the newly derived data. Also, only individuals who have been appointed, trained, and certified as PIV Officials (PCI Managers, Sponsors, Registrars, or Issuers) may access the VA PIV Enrollment Portal. The facility PCI Manager is the appropriate point of contact for all information related to certification of system officials and access to the VA PIV Enrollment Portal. A PIV card is required to gain access to the VA PIV Enrollment Portal. There is no analysis conducted by VACO – PIV Assessing.

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?

VACO - PIV Assessing protects data by using the 140-2 encryption method, two-factor authentication, a time-out function after 30 minutes of activity, the logging of all computer-readable data extracts containing sensitive information, and the removal of those data extracts from the device within 90 days or when its use is no longer required.

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

The controls in place ensure that information is handled appropriately are a part of numerous NIST families including, but not necessarily limited to, Access Control (AC), Planning (PL) and Security Assessment and Authorization (CA). The applicants are required to complete a Rules of Behavior (RoB) form and the Security Awareness Training (SAT) on an annual basis. Both will provide the applicants with the guidance needed for the appropriate use of the information. SSNs are encrypted with FIPS 199 compliant method of encryption.

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

Access to the PII contained in VACO-PIV Assessing is based on the principle of least privileg more commonly referred to as "need-to-know." The need-to-know is determined by everyone's job position and by the supervisors within the employees' chain of command. System officials will have access to only the information that is required for the performance of their job duties. System Administrators, Managers, Supervisors, and Moderators are operating under the same rules of behavior for the VA and Federal Employees in terms of protecting the privacy of others and not using information in the system for personal gain or for the benefit of others. Passwords, user IDs, and segmentation of function provide adequate protections.

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 PII contained in VACO-PIV Assessing is based on the principle of least privilege, more commonly referred to as "need-to-know." The need-to-know is determined by everyone's job

position and by the supervisors within the employees' chain of command. System officials will have access to only the information that is required for the performance of their job duties. System Administrators, Managers, Supervisors, and Moderators are operating under the same rules of behavior for the VA and Federal Employees in terms of protecting the privacy of others and not using information in the system for personal gain or for the benefit of others. Passwords, user IDs, and segmentation of function provide adequate protections.

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

The controls in place ensure that information is handled appropriately are a part of numerous NIST families including, but not necessarily limited to, Access Control (AC), Planning (PL) and Security Assessment and Authorization (CA). The applicants are required to complete a Rules of Behavior (RoB) form and the Security Awareness Training (SAT) on an annual basis. Both will provide the applicants with the guidance needed for the appropriate use of the information.

2.4c Does access require manager approval?

The VACO-PIV Assessing Program Manager approves all accesses to the system. Physical access to the system is enforced by requiring presentation of a valid ID card before gaining access to the data center.

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

Our facilities employ all security controls in the respective high impact security control baseline unless specific expectations have been allowed based on the tailoring guidance provided in NIST Special Publication 800-53 and specific VA directives.

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

System officials will have access to only the information that is required for the performance of their job duties. System Administrators, Managers, Supervisors, and Moderators are operating under the same rules of behavior for the VA and Federal Employees in terms of protecting the privacy of others and not using information in the system for personal gain or for the benefit of others. Passwords, user IDs, and segmentation of function provide adequate protections.

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*

Full Name
SSN
DoB

Mailing Address
Zip Code
Phone Number
Email
Mother's maiden name
Emergency Contact
Race
Passport Number
Driver's License
Taxpayers Identification Number
Fingerprints
Photographic Image

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. 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 are retained in accordance with records retention standards approved by the Archivist of the United States, the National Archives and Records Administration (NARA), and published in Agency Records Control Schedules. Records are destroyed upon notification of death or not later than five years after separation or transfer of employee, whichever is applicable. Audit logs which describe a security breach must be maintained for 6 years as required by HIPAA requirements.

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?

Yes, they are in (https://www.archives.gov/files/records-mgmt/grs/grs05-6.pdf) as approved by NARA

3.3b Please indicate each records retention schedule, series, and disposition authority The PIV records are retained in accordance with the General Records Schedule 5.6 item 181 and disposition schedule *##DAA-GRS2021-0001-0008*

(https://www.archives.gov/files/records-mgmt/grs/grs05-6.pdf) as approved by NARA

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.

When the PIV system owner determines that data is no longer needed and there is no requirement for them to be retained, records are destroyed on-site in a manner commensurate with the medium on which they were stored. Paper documents are destroyed to an unreadable state in accordance with the Department of Veterans' Affairs VA Directive 6371, (April 8, 2014) (https://www.va.gov/vapubs/viewPublication.asp?Pub_ID=742&FType=2)
Electronic data and files of any type, including Protected Health Information (PHI), Sensitive Personal Information (SPI), Human Resources records, and more are destroyed in accordance with the **Department of Veterans' Affairs Directive 6500** (https://www.va.gov/digitalstrategy/docs/VA_Directive_6500_24_Jan_2019.pdf).
When required, this data is deleted from their file location and then permanently deleted from the deleted items or Recycle bin. Magnetic media is wiped and sent out for destruction per VA Directive 6500. Digital media is shredded or sent out for destruction per VA Directive 6500.

Automated storage media is retained and disposed of in accordance with deposition authorization approved by the Archivist of the United States. The authorized destruction of records that are restricted from disclosure by statute, such as PA or Title 38 U.S.C., must be witnessed by a federal employee or a contractor employee. If a contract is used to dispose of restricted VA records, the facility Records Officer must authorize the use of a contractor or subcontractor employee to witness the destruction. Additionally, this system follows Field Security Service (FSS) Bulletin #176 dated April 9, 2014, for Media Sanitization Program, SOPs - FSS - All Documents as well as FSS Standard Operating Procedures (SOP) MP-6 Electronic Media Sanitization.
The VA requires that the destruction of national security-related information, including the method of destruction, must be approved by the VA Security Officer, Office of the Assistant Secretary for Security and Law Enforcement. Any contract for sale of VA records must prohibit their resale for use as records or documents. PIV records are destroyed at VA owned facilities.

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.

VACO-PIV Assessing does utilize techniques to minimize the risk to privacy of using PII for research, testing, and training when feasible. VACO-PIV Assessing utilizes dummy data for research, training, and testing whenever possible. VACO-PIV Assessing utilizes NO real data in non-production environments – Development, Test, and Pre-Production. We utilize generated data to include dummy PIV cards filled with deidentified data.

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: There is a risk if the VACO – PIV Assessing System retains information collected longer than its required period of five years as stated by NARA, as well as the Audit logs which describe a security breach for over six years as required by HIPAA requirements. The longer a project retains information, the longer it needs to secure the information and assure its accuracy and integrity.

Mitigation: To mitigate the risk posed by information retention, VACO-PIV Assessing adheres to the VA Readjustment Counseling Service (RCS) schedules for each category of data it maintains. When the retention data is reached for a record, VACO-PIV Assessing will then carefully dispose of data by the appropriate method.

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***
OI&T/Identity Access Management (IAM)	PII is shared with IAM for Single Sign On efforts	Full Name SSN DoB Mailing Address Zip Code Phone Number Email Mother's maiden name Emergency Contact Race Passport Number Driver's License Taxpayers Identification Number Fingerprints Photographic Image	Security Attribute Mark-up Language (SAML)

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: There is a risk that information may be shared with an unauthorized VA program, system, or individual.

Mitigation: Safeguards implemented to ensure data is not sent to the wrong VA organization include employee security and privacy training and awareness and required reporting of suspicious activity. Use of PIV cards for physical access to facilities and logical access to user accounts, Personal Identification Numbers (PINs), access to information only on a need-to-know basis, encryption, and access authorization using Network Identification (NTID) are all measures that are utilized within the VACO-PIV Assessing facilities.

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***
Verizon Business Shared Service System	VACO-PIV Assessing utilizes Verizon Business's PKI Service in accordance with the steps laid out in OMB M-05-24. It utilizes the PKI service to remain compliant with FIPS 201.	Full Name SSN DoB Mailing Address Zip Code Phone Number Email Mother's maiden name Emergency Contact Race Passport Number Driver's License Taxpayers Identification Number Fingerprints Photographic Image	Privacy Act of 1974, 5 U.S.C. § 552a Health Insurance Portability and Accountability Act (HIPAA) Security Rule, 45 C.F.R. Parts 160, 164 Confidential Nature of Claims, 38 U.S.C § 5701 Freedom of Information Act, 5 U.S.C. § 552 VA Directive and Handbook 6500, Information Security Program National Institute of Standards and Technology (NIST) Special Publication (SP) 800-47, Interconnecting Information Technology Systems SORN ID# 145VA005Q3 Interconnection Security Agreement and Memorandum of Understanding Between VA PIV Operations, CRRC, HITC, and Verizon	The transmission takes place electronically. The connection between the PIV system and Verizon Business PKI service is secured by utilizing TLS and is initiated from with the CMS product through an interface via a UPI connector. The connector communicates with the Certificate Authority (CA) service via an x.509 certificate authentication mechanism. The CMS is connected to the Hardware Security Module (HSM) that contains and

			Business, v2.1 (May 3, 2018)	controls cryptographic material which is used to authenticate and secure all data

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.

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: There is a risk if information may be accidentally shared with or maliciously disclosed to an unauthorized entity outside the VA.

Mitigation: The safeguards implemented to ensure data is not accidentally or maliciously shared with an unauthorized organization or entity include employee security awareness and privacy training which occurs on no less frequently than annually and required reporting of suspicious activity. The use of PIV cards for physical access and PIV cards with PINs for logical access, access to data only on a need-to-know basis, and the encryption of data at rest are all measures that are utilized within the facilities and by remote users.

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.

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

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. This question is 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.

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

The only way PII is collected is directly from the applicant via Form 0711 OMB No. 2900-0673, *Request for Personal Identity Verification Card*. A notice is provided to the applicant on that form. The applicant's only responsibility is to read the notice and fill out this form. The applicant must fill out the form and submit it to initiate the process of obtaining a PIV Card. Failure to provide all the requested information on the form may result in the VA being unable to process the applicant's request for a PIV card or denial of issuance of a PIV card. The Privacy Act statement is a part of all VA forms, and it is explained prior to the applicant signing any documents. The Privacy Action Notice and the SORN are attached in Appendix A.

A copy of this form is located at
http://www.va.gov/OPTOMETRY/docs/vaform0711reqforidverificationcard.pdf.

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.

Additional notice is provided through this PIA, which is available online as required by the eGovernment Act of 2002, Public Law 107-347 §208(b)(1)(B)(iii), the Department of Veterans Affairs, the VA SORN (ID # 145VA005Q3), and the VA SORN (ID # 103VA07B) which are published in the Federal Register and available online. The SORNs can be viewed and accessed by clicking on the following link: https://www.oprm.va.gov/privacy/systems_of_records.aspx. A copy of the Notice of Privacy Practices is also attached in Appendix A.

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.

The applicants could decline to provide the information requested on Form 0711 OMB No. 2900-0673. However, failure to provide all the requested information may result in the VA being unable to process the request or denial of issuance of a PIV card, and since PIV cards grant both physical access to VA facilities and logical access to VA networks, it is likely that it will impact the applicant's status as a VA employee, contractor, or affiliate.

6.3 Do individuals have the right to consent to 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.

Individuals may provide consent which covers all uses (current and potential) of his or her information. Providing consent for all uses and not for others is not allowed.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

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 Privacy risk is not providing a Privacy Notice to individuals upon collection of their personal information.

Mitigation VACO-PIV Assessing mitigates this risk by ensuring that it provides individuals with notice of information collection and notice of the system's existence through the methods discussed in question 6.1.

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.

SORN145VA005Q3; RECORD ACCESS PROCEDURES: Individuals seeking information on the existence and content of records in this system pertaining to them should contact the system manager in writing as indicated above. A request for access to records must contain the requester's full name, address, telephone number, be signed by the requester, and describe the records sought in sufficient detail to enable VA personnel to locate them with a reasonable amount of effort.

SORN103VA07B; RECORD ACCESS PROCEDURES: Individuals seeking information on the existence and content of records in this system pertaining to them should write, call or visit the VA facility where the records are maintained.

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.

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).

SORN 103VA07B; "Police and Security Records-ID-VA is exempt VA Privacy Act system of records (see, 38 CFR 1.582) FOR FURTHER INFORMATION CONTACT:
Director Police and Security Service
(07B), Department of Veterans Affairs,
810 Vermont Avenue NW., Washington,
DC 20420, telephone (202) 273–5544. Link: 03-14861.pdf (govinfo.gov)
https://www.govinfo.gov/content/pkg/FR-2003-06-13/pdf/03-14861.pdf

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

SORN145VA005Q3; RECORD ACCESS PROCEDURES: Individuals seeking information on the existence and content of records in this system pertaining to them should contact the system manager in writing as indicated above. A request for access to records must contain the requester's full name, address, telephone number, be signed by the requester, and describe the records sought in sufficient detail to enable VA personnel to locate them with a reasonable amount of effort.

SORN103VA07B; RECORD ACCESS PROCEDURES: Individuals seeking information on the existence and content of records in this system pertaining to them should write, call or visit the VA facility where the records are maintained.

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.

SORN
103VA07B; "Police and Security Records-ID-VA
145VA005Q3; "Department of Veterans Affairs Personnel Security File System (VAPSFS)-VA"

(https://www.oprm.va.gov/privacy/systems_of_records.aspx).
https://www.govinfo.gov/content/pkg/FR-2022-07-01/pdf/2022-14118.pdf

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.

SORN145VA005Q3; RECORD ACCESS PROCEDURES: Individuals seeking information on the existence and content of records in this system pertaining to them should contact the system manager in writing as indicated above. A request for access to records must contain the requester's full name, address, telephone number, be signed by the requester, and describe the records sought in sufficient detail to enable VA personnel to locate them with a reasonable amount of effort.

SORN103VA07B; RECORD ACCESS PROCEDURES: Individuals seeking information on the existence and content of records in this system pertaining to them should write, call or visit the VA facility where the records are maintained.

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 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.

SORN145VA005Q3; RECORD ACCESS PROCEDURES: Individuals seeking information on the existence and content of records in this system pertaining to them should contact the system manager in writing as indicated above. A request for access to records must contain the requester's full name, address, telephone number, be signed by the requester, and describe the records sought in sufficient detail to enable VA personnel to locate them with a reasonable amount of effort.

SORN103VA07B; RECORD ACCESS PROCEDURES: Individuals seeking information on the existence and content of records in this system pertaining to them should write, call or visit the VA facility where the records 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 can 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: There is a risk that the subjects of the records within the system will not know the relevant procedures for gaining access to, correcting, or contesting their information.

Mitigation: Information provided during the PIV application process is verified by the registrar. If data is found to be missing or inaccurate, the data registrar working on the application will contact the employee/contractor and notify them, this will provide the employee the opportunity to resubmit the required documentation. Applicable SORN or the Notice is located in Appendix A.

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.

A user may have “read-only” access but will not be able to make any changes to the provided information. For additional information see the VACO-PIV Assessing SSP and the AC Access control Implementation statements.

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?

There are no users from other agencies who may have access to the system.
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.

User roles for the VACO-PIV Assessing system include:

PIV Manager/Sponsor- The authoritative VACO-PIV Assessing role that validates and substantiates the card applicant's need for an identification card; initiates the appropriate background investigation process; and provides the demographic and organizational data required to move the enrollment process forward.

PIV Registrar – The authoritative VACO-PIV Assessing role that collects demographic and biometric information and identity proofs the card applicant based on I-9 Form standard identification source documents.

PIV Issuer – The authoritative VACO-PIV Assessing role that validates the identity of the card applicant, produces the identification card, and issues the credential to the new user.

PCI Manager – The administrative authority for all VACO-PIV Assessing roles.

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.

Yes, contractors do have access to the system and the PII. Contractors and sub-contractors must sign the VA Contractors ROB. The ROB are enforced for all VA system users to ensure appropriate use and protection of the information. The ROB are reviewed and resigned by each user on an annual basis. Contractors and sub-contractor access is reviewed by the VACO-PIV Assessing system owner no less frequently than annually to determine who still requires access to the system as well as the type of access rights needed based on the specific job duties and need to know. The contractor ROB can be found in TMS 10176 or Appendix A to VA Handbook 6500.6. All contractors sign the Non-Disclosure Agreement according to the Acceptable Use Policy (AUP).

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

Personnel who will be accessing information systems must read and acknowledge their receipt and acceptance of the VA Information Security Rules of Behavior (RoB) prior to gaining access to any VA information system or sensitive information. The rules are included as part of the security awareness training that all personnel must complete via the VA's TMS. After the DAPER 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. This training includes, but is not limited to, the following TMS Courses:

. 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
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

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

8.4a If yes, provide:

1. *The Security Plan Status:* Authorization to Operate (ATO)
2. *The System Security Plan Status Date: January 7, 2021*
3. *The Authorization Status:* Authorization to Operate (ATO)
4. *The Authorization Date:* January 7, 2021
5. *The Authorization Termination Date:* January 7, 2024
6. *The Risk Review Completion Date:* December 8, 2020
7. *The FIPS 199 classification of the system:* Moderate

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

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

N/A

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 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)*

This System does not use Cloud.

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.*

This System does not use Cloud

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.

This System does not use Cloud

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.

This System does not use Cloud

9.4 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).

This System does not use Cloud

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
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

ID	Privacy Controls
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 provided in this Privacy Impact Assessment is true and accurate.

JULIE C. DRAKE 969177

Digitally signed by JULIE C. DRAKE 969177
Date: 2023.02.10 16:40:38 -07'00'

Privacy Officer, Julie Drake

DEREK STERNS

Digitally signed by DEREK STERNS
Date: 2023.02.13 08:07:35 -05'00'

Information Systems Security Officer, Derek Sterns

JASON MILLER

Digitally signed by JASON MILLER
Date: 2023.02.13 15:20:28 -06'00'

Information Systems Owner, Jason Miller

APPENDIX A-6.1

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).

VA Form 0711, Oct 2006

PRIVACY ACT STATEMENT: VA is authorized to ask for the information requested on this form by Homeland Security Presidential Directive (HSPD)-12, and 31 USC 7701. The information and biometrics collected, collected as part of the Federal identity-proofing program under HSPD-12 are used to verify the personal identity of VA applicants for employment, employees, contractors, and affiliates (such as students, WOC employees, and others) prior to issuing a department identification credential. The credentials themselves are to be used to authenticate electronic access requests from VA employees, contractors, and affiliates issued a department identification credential to gain access to VA facilities and networks (where available) through digital access control systems, as well as to other federal government agency facilities and systems were permitted by law. The information collected on this form is protected by the Privacy Act, 5 USC Section 552(a) and maintained under the authority of 38 USC Section 501 and 38 USC Sections 901-905 in VA system of records "Police and Security Records-VA (103VA07B)". VA may make a "routine use" disclosure of the information in this system of records for the routine uses listed in this system of records, including civil or criminal law enforcement, constituent congressional communications initiated at your request, litigation or administrative proceedings in which the United States is a party or has an interest, the administration of VA programs, verification of identity and status, and personnel administration by Federal agencies. Failure to provide all of the requested information may result in VA being unable to process your request for a Personal Identity Verification Card, or denial of issuance of a Personal Identity Verification Card. If you do not have a Personal Identity Verification Card, you may not be granted access to VA facilities or networks, which could have an adverse impact on your application to become, or status as, a VA employee, contractor, or affiliate where such access is required to perform your assigned duties or responsibilities.

PAPERWORK REDUCTION ACT NOTICE: The public reporting burden is approximately 5 minutes including time to review instruction, find the information, and complete this form. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to the VA Clearance Officer (005E3), 810 Vermont Avenue, Washington, DC 20420.

HELPFUL LINKS:

Record Control Schedules:

https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf

General Records Schedule 1.1: Financial Management and Reporting Records (FSC):

https://www.archives.gov/files/records-mgmt/grs/grs01-1.pdf

National Archives (Federal Records Management):

https://www.archives.gov/records-mgmt/grs

VHA Publications:

https://www.va.gov/vhapublications/publications.cfm?Pub=2

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