Privacy Impact Assessment for the VA IT System called:

Veterans Re-Entry Search Service (VRSS)
Veterans Health Administration (VHA)
VA Homeless Program Office

Date PIA submitted for review:

5/23/2023

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Phillip Cauthers	Phillip.Cauthers@va.gov	503-721-1037
Information System Security Officer (ISSO)	James Alden	james.alden@va.gov	781-687-2768
Information System Owner	Temperance Leister	temperance.leister@va.gov	484-432-6161

Abstract

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

The Department of Veterans Affairs (VA) has aggressively undertaken an initiative to end homelessness among Veterans by developing new prevention initiatives and expanding existing programs to provide shelter and comprehensive supportive services for homeless Veterans. The Veteran Re-entry Search Service (VRSS) project will identify veterans who are incarcerated in correctional facilities nationwide. VRSS will interact with Federal, State and Local correctional facilities and courts providing confirmation an individual is a veteran.

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.

Veterans Re-Entry Search Service (VRSS)
VA Homeless Program Office

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

The Veterans Re-Entry Search Service (VRSS) is an automated system used to identify Veterans who are incarcerated or under supervision in the courts. VA does not have enough resources to personally contact all identified incarcerated Veterans, so correctional facility staff can assist with referrals to Veteran services. Some correctional facilities provide Veterans special services and/or are co-locating Veterans in special units. Information about incarcerated Veterans provided by VRSS is used by the Veterans Justice Outreach (VJO) and the Healthcare for Re-entry Veterans (HCRV) organizations as part of their outreach activities to prevent Veteran homelessness. HCRV is designed to address community reentry needs of incarcerated Veterans; it reduces the impact of medical, psychiatric, and substance abuse problems upon community readjustment to decrease the likelihood of re-incarceration for those leaving prison. VJO provides outreach and linkage to VA services for Veterans at early stages of the justice system, including Veterans' courts, drug courts, and mental health courts.

All users interact with VRSS using a secure web browser. VRSS allows correctional facilities and other justice systems, including courts to upload inmate data pertaining to their incarcerated, detained, or court docket population. VRSS then interfaces with the Veterans Affairs/Department of Defense Identity Repository (VADIR) to identify any Veterans from those lists. An electronic listing of Veterans and their probable eligibility status is transmitted back to the originating correctional facility/court system (CF/CS) in order to facilitate outreach by correctional/court staff with

incarcerated Veterans. Functionality is also being developed with the DAS (Data Access Services) Gateway. DAS Gateway will act as a proxy to automate the process by which the incarcerated population data is pulled from the CF/CS. Existing or new CF/CS entities that wish to participate using this automated process will complete all VLER DAS requirements prior to interfacing with the DAS Gateway.

Approximate number of records expected to be stored in this system is 100,000 to 200,000. Title 38, United States Code, Section 501 is the legal authority for operation/maintenance of this system.

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

Veterans Re-Entry Search Service (VRSS) is owned by the Veterans Health Administration (VHA) Programs Office.

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.*

Approximate number of records expected to be stored in this system is 100,000 to 200,000. Title 38, United States Code, Section 501 is the legal authority for operation/maintenance of this system.

The Veterans Re-Entry Search Service (VRSS) is an automated system used to identify Veterans who are incarcerated or under supervision in the courts. VA does not have enough resources to personally contact all identified incarcerated Veterans so correctional facility staff can assist with referrals to Veteran services.

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

The Veterans Re-Entry Search Service (VRSS) is an automated system used to identify Veterans who are incarcerated or under supervision in the courts. VA does not have enough resources to personally contact all identified incarcerated Veterans, so correctional facility staff can assist with referrals to Veteran services. Some correctional facilities provide Veterans special services and/or are co-locating Veterans in special units. Information about incarcerated Veterans provided by VRSS is used by the Veterans Justice Outreach (VJO) and the Healthcare for Re-entry Veterans (HCRV) organizations as part of their outreach activities to prevent Veteran homelessness

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

Information about incarcerated Veterans provided by VRSS is used by the Veterans Justice Outreach (VJO) and the Healthcare for Re-entry Veterans (HCRV) organizations as part of their outreach activities to prevent Veteran homelessness. HCRV is designed to address community re-entry needs of incarcerated Veterans; it reduces the impact of medical, psychiatric, and substance abuse problems upon community readjustment to decrease the likelihood of re-incarceration for

those leaving prison. VJO provides outreach and linkage to VA services for Veterans at early stages of the justice system, including Veterans' courts, drug courts, and mental health courts.

3. Legal Authority and SORN

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

Title 38, United States Code, Section 501 is the legal authority for operation/maintenance of this system. Title 10 U.S.C. chapters 106a, 510, 1606 and 1607 and Title 38, U.S.C. Sections 501(a), 1710, 1729 and Section 7304, Chapters 11, 13, 15, 18, 23, 30, 31, 32, 33, 34, 35, 36, 39, 51, 53, and 55 provide

the legal authority for operating the VRSS system. Authority is from Title 38, United States Code, Section 5106 – Furnishing of information by other agencies. Public Law 99-272, Consolidated Omnibus Budget Reconciliation Act of 1985, enacted April 7, 1986. Public Law 110-387, Veterans' Mental Health and Other Care Improvements Act of 2008. Sharing of information between VA and correctional institutions is permitted according to 38 United

States Code (USC) Sec. 5106; it permits other agencies to provide VA information for the purposes of determining eligibility. Public Law 107-95 allows identification and contacting of Veterans who are homeless or at risk of homelessness as well as coordination of services provided to Veterans with services provided by those organizations. Sharing of information between VA and correctional institutions will be determined for legal authority under the Privacy Act once the Privacy Act system of records for which the information will be maintained is made. 38 U.S.C. Sec. 5701(f) allows for disclosure to any nonprofit organization if the release is directly connected with the conduct of programs and the utilization of benefits Disclosure of information derived from VHA would also be governed by the Health Insurance Portability and Accountability Act (HIPAA Privacy Rule, 45 U.S.C. 164.512) and an appropriate exception identified.

(https://www.oprm.va.gov/privacy/systems_of_records.aspx).

The Authority for this system is derived from SORN 121VA10 "National Patient Databases-VA", Title 38 United States Code Section 501. https://www.govinfo.gov/content/pkg/FR-2023-04-12/pdf/2023-07638.pdf

H. 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?

N/A

D. System Changes

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

No

J. Whether 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.

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)

- User Name
- User Email
- User Phone
- User Password
- User Login Number
- User Account Type
- User Correctional System ID
- User Register Date
- User Status
- Prisoner/Defendant ID Number
- Cell Location
- Facility/Court Name
- Facility/Court Zip Code
- Facility/Court State
- Parole Date
- Release or Hearing Date

PII Mapping of Components (Servers/Database)

VRSS 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 VRSS 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	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards

		PII? (Yes/No)			
Database 1	Yes	Yes	Name Social Security Date Of Birth Personal Email Race/Ethnicity Prisoner/ Defendant ID Number Cell Location Facility/Court Zip Code Facility/Court State Parole Date Release or Hearing Date	To identify Veterans who are incarcerated or under supervision in the courts	Database is encrypted. Utilizes https; Multiple layered security (firewall; web application firewall)

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?

Correctional facilities/court systems (CF/CS) upload inmate data pertaining to their incarcerated, detained, or court docket population to VRSS. VRSS then interfaces with the Veterans Affairs/Department of Defense Identity Repository (VADIR) to identify any Veterans from those lists. An electronic listing of Veterans and their probable eligibility status is transmitted back to the originating correctional facility/court system (CF/CS) in order to facilitate outreach by correctional/court staff with incarcerated Veterans.

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.

Correctional facilities/court systems (CF/CS) upload inmate data pertaining to their incarcerated, detained, or court docket population to VRSS. VRSS then interfaces with the Veterans Affairs/Department of Defense Identity Repository (VADIR) to identify any Veterans from those lists. An electronic listing of Veterans and their probable eligibility status is transmitted back to the originating correctional facility/court system (CF/CS) in order to facilitate outreach by correctional/court staff with incarcerated Veterans.

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

N/A

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?

VRSS does not collect data directly from the Veterans. Correctional facilities/court systems (CF/CS) upload inmate data pertaining to their incarcerated, detained, or court docket population directly into VRSS via electronic file transfer.

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.

N/A

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.

The purpose of the data collected by VRSS is to:
• Provide VA with accurate information about incarcerated Veterans.
• Allow HCRV and JVO Specialists are to provide incarcerated Veterans outreach services.
• Facilitate enrollment and access to VA services by incarcerated Veterans.
• Enable correctional facilities/court systems to plan services for Veterans in their populations.
• Enable correctional facilities/court systems to support VA outreach activities.
• Enable correctional facilities/court systems to support enrollment and access to services by incarcerated Veterans.

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.

The VRSS interface allows CF/CS users upload .csv files to the VRSS web application using their existing workstations and associated peripherals used for data entry. The DAS Gateway will automate this upload process. The data files uploaded to VRSS must comply with the VRSS File Format Standards and Specifications document. A few key requirements are:
• Files must be in comma-separated value (.csv) format
• Files must contain fourteen (14) distinct fields (as listed in section 1.1).
• If required fields contain partial or no data for a particular individual VRSS will reject the entire file.

The VRSS application contains a data validation module that verifies and validates the contents of the files uploaded which must comply with established file format and specifications for each of the available fields. CF/CS users are able to perform a preliminary file validation when initially uploading their .csv file. If the file deviates from the prescribed file format specifications, the users receive a negative file validation error with noted discrepancies. Users can then make corrections and check the file again. Once all negative validation issues have been addressed then a positive file validation message will be displayed, and the user can proceed to upload the file for transfer.

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

Title 38, United States Code, Section 501 is the legal authority for operation/maintenance of this system.
Title 10 U.S.C. chapters 106a, 510, 1606 and 1607 and Title 38, U.S.C. Sections 501(a), 1710, 1729 and Section 7304, Chapters 11, 13, 15, 18, 23, 30, 31, 32, 33, 34, 35, 36, 39, 51, 53, and 55 provide the legal authority for operating the VRSS system. Authority is from Title 38, United States Code, Section 5106 – Furnishing of information by other agencies.
Public Law 99-272, Consolidated Omnibus Budget Reconciliation Act of 1985, enacted April 7, 1986.
Public Law 110-387, Veterans' Mental Health and Other Care Improvements Act of 2008.
Sharing of information between VA and correctional institutions is permitted according to 38 United States Code (USC) Sec. 5106; it permits other agencies to provide VA information for the purposes of determining eligibility.
Public Law 107-95 allows identification and contacting of Veterans who
are homeless or at risk of homelessness as well as coordination of services provided to Veterans with services provided by those organizations. Sharing of information between VA and correctional institutions will be determined for legal authority under the Privacy Act once the Privacy Act system of records for which the information will be maintained is made. 38 U.S.C. Sec. 5701(f) allows for disclosure to any nonprofit organization if the release is directly connected with the conduct of

programs and the utilization of benefits Disclosure of information derived from VHA would also be governed by the Health Insurance Portability and Accountability Act (HIPAA Privacy Rule, 45 U.S.C. 164.512) and an appropriate exception identified.

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:
VRSS collects Sensitive Personal Information (SPI) to identify individuals as veterans for use by VJO and HCRV programs. If this information was breached or accidentally released to inappropriate parties or the public, it could result in financial, personal, and/or emotional harm to the individuals whose information is contained in the system.

Mitigation:
The Department of Veterans Affairs is careful to only collect the information necessary to identify an individual as a veteran. By only collecting the minimum necessary information, the VA is able to better protect the individual's information and reduce the risk. Access is restricted to VA approved users. Users of this system are vetted by Veterans Justice Outreach (VJO) and Healthcare for Re-entry Veterans (HCRV) organizations through contacts of facility administrator from outreach state representatives procedures. Each user must take VA Privacy and Information Security Rules of Behavior training (or VA approved equivalent) annually to maintain access.

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.

VRSS business benefits include the following capabilities:
• Provide VA with accurate information about incarcerated Veterans.
• Allow HCRV and JVO Specialists are to provide incarcerated Veterans outreach services.
• Facilitate enrollment and access to VA services by incarcerated Veterans.
• Enable correctional facilities/court systems to plan services for Veterans in their populations.
• Enable correctional facilities/court systems to support VA outreach activities.
• Enable correctional facilities/court systems to support enrollment and access to services by incarcerated Veterans.

o First Name - Veteran's identification -internal
o Middle Name - Veteran's identification-internal
o Last Name - Veteran's identification-internal
o Suffix Name - Veteran's identification-internal
o SSN - Veteran's identification-internal
o Date of Birth - Veteran's identification -internal
o Gender - Veteran's identification-internal
o Prisoner/Defendant ID Number - Individual identification to be used when returning results of the Veteran search conducted by VRSS- external
o Cell Location - cell location identifier- external
o Facility/Court Name - Facility/Court identification to be used when returning results of the Veteran search conducted by VRSS- external
o Facility/Court Zip Code - Facility/Court identification-internal/external
o Facility/Court State - Facility/Court identification-internal/external
o Parole Date - Parole date identification-internal/external
o Release or Hearing Date - Actual or projected release date identification-internal/external

• The following information is provided by CF/CS employees or produced by VRSS:
o User Name – used for CF/CS employee identification VRSS user account – internal
o User Email– used for CF/CS employee identification VRSS user account – internal
o User Phone- used to communicate with user- internal
o User Password- user account administration - internal
o User Login Number– used for CF/CS employee authentication VRSS user account – internal
o User Account Type– used for CF/CS employee authentication VRSS user account – internal
o User Correctional System ID– used for CF/CS employee authentication VRSS user account – internal
o User Register Date – used for CF/CS employee authentication VRSS user account – internal
o User Status– used for CF/CS employee authentication VRSS user account – internal

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.

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.

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.

VRSS provides a secure web interface that allows correctional facilities and other justice systems, including courts to upload inmate data pertaining to their incarcerated, detained, or court docket population. VRSS then interfaces with the Veterans Affairs/Department of Defense Identity Repository (VADIR) to identify any Veterans from those lists. Data uploaded by the correctional facilities/court systems (CF/CS) is transferred from VRSS to VADIR, where a matching algorithm attempts to identify possible Veterans. An electronic listing of Veterans and their probable eligibility status is transmitted back to the originating correctional facility/court system (CF/CS) in order to facilitate outreach by correctional/court staff with incarcerated Veterans. Functionality is also being developed with the DAS (Data Access Services) Gateway. DAS Gateway will act as a proxy to automate the process by which VRSS pulls the incarcerated population data and then automatically returns the file containing only identified Veterans. Existing or new CF/CS entities that wish to participate will complete all required VLER DAS requirements prior to interfacing with the DAS Gateway.

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?

Encryption
Utilizes https; Multiple layered security (firewall; web application firewall)

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

Encryption
Utilizes https; Multiple layered security (firewall; web application firewall)

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

Encryption
Utilizes https; Multiple layered security (firewall; web application firewall)

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.

How is access to the PII determined?

Are criteria, procedures, controls, and responsibilities regarding access documented?
Does access require manager approval?
Is access to the PII being monitored, tracked, or recorded?
Who is responsible for assuring safeguards for the PII?

The VA Homeless Veterans Health Care for Re-entry Veterans (HCRV) webpage provides users with program information and guidance/training at http://www.va.gov/homeless/Reentry.asp
The System of Record Notice (SORN) that applies to this system defines the information collected from veterans, use of the information, and how the information is accessed and stored.
The information collected by this system falls under System of Record Notice (SORN) 121VA10-National Patient Databases-VA. This SORN can be found online at
https://www.govinfo.gov/content/pkg/FR-2023-04-12/pdf/2023-07638.pdf

The minimum security requirements for VRSS high impact system cover 17 security-related areas

with regard to protecting the confidentiality, integrity, and availability of VA information systems and the information processed, stored, and transmitted by those systems. The security related areas include: access control; awareness and training; audit and accountability; certification, accreditation, and security assessments; configuration management; contingency planning; identification and authentication; incident response; maintenance; media protection; physical and environmental protection; planning; personnel security; risk assessment; systems and services acquisition; system and communications protection; and system and information integrity. The VRSS application team has implemented the required security controls based on the tailoring guidance of NIST Special Publication 800-53 and VA directives or handbooks. VA Records Management Policy and VA Directives or Handbooks govern how veterans' information is used, stored, and protected.
Users are trained how to handle sensitive information by taking VA Privacy and security awareness training and reading and attesting they understand the VA Rules of Behavior or VA approved equivalents. VA does have a reciprocity agreement for accepting other government agency training completion provided the course meets VA standards.

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*

VRSS only retains information for those Veteran matches identified by VADIR:
• First Name
• Middle Name
• Last Name
• Suffix Name
• SSN
• Date of Birth
• Gender
• Prisoner/Defendant ID Number
• Cell Location
• Facility/Court Name
• Facility/Court Zip Code
• Facility/Court State
• Parole Date
• Release or Hearing Date
The VA also retains the following CF/CS employee data:
• User Name
• User Email
• User Phone
• User Password

• User Login Number
• User Account Type
• User Correctional System ID
• User Register Date
• User Status

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.*

VRSS program personnel intend to set the retention period for VRSS output files at 30 days (for files generated by Court System users)/60 days (for files generated by Correctional Facility users), with both the original submission and the VA generated results files being deleted after those periods.

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?

Records Control Schedule GRS 5.2 020 has been approved by NARA.
https://www.archives.gov/files/records-mgmt/grs/grs05-2.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.

Electronic media sanitization, when the records are authorized for destruction (or upon system decommission) will be carried out in accordance with VA 6500.1 HB Electronic Media Sanitization. Disposition of Printed Data: Forms and other types of printed output produced by any computer systems and related peripherals will be evaluated by the responsible staff member for data sensitivity. Printed output containing sensitive data will be stored in locked cabinets or desks, and disposed of properly by shredding or similar VA approved methods in accordance with VA Directive 6371. Program listings and documentation relating to the use of or access to a computer system require special handling if the listings or documentation provide information about a system which processes sensitive data. VA personnel are responsible for retrieving/removing all printed outputs they request from printers

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.

VRSS resides on a production, pre-production, and development environment. The production environment handles PHI/PII data; preproduction is used for staging the application after new releases/changes and before deploying to production; access to the development environment is strictly limited to the application developers. The VRSS program follows the guidance provided by the Veteran-Focused Integration Process (VIP), and agreed upon requirements are worked and tested before the application is released to production. User testing may also take place as part of a new version release, depending on the extent of the changes. In addition, VHA programs may need to train staff on functionality in the new or modified IT system. Training, including on IT systems, is part of health care operations and per VHA policy PII and PHI may be used for that training purpose. However, VHA must minimize the use of PII and PHI in training presentations or materials per VA Directive 6511.

3.6 <u>PRIVACY IMPACT ASSESSMENT: Retention of information</u>

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 that the information maintained by VRSS could be retained for longer than is necessary to fulfill the VA mission. Records held longer than required are at greater risk of being unintentionally released or breached.

Mitigation:
To mitigate the risk posed by information retention, VRSS adheres to the Records Schedule approved by NARA. When the retention date is reached for a record, the individual's information is carefully disposed of by the determined method as described in Records Schedule in accordance with VA media destruction policies.

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

Identify and list the names of any VA program offices, other VA organizations or IT systems <u>within</u> VA with which information is shared	**Specifically list the Data Elements**	**Method of Transmission**
Veterans Health Administration (VHAAdministration	Name, SSN, Date of Birth, Gender, Race/Ethnicity, Prisoner/Defendant ID Number, Cell Location, Facility/Court Name, Facility/Court Zip Code, Facility State, Parole Date, Release/Hearing Date, User Name, User Email, User Phone, User Password, User Login Number, User Account Type, User Correctional System ID, User Register Date, User Status	Secure electronic file via Secure Hypertext Transfer Protocol (HTTPS)/Single Socket Layer (SSL) as standard security technology for establishing an encrypted link between a web server and a browser transfer.
Veterans Justice Outreach (VJO) program. VJO provides outreach and linkage to VA services for Veterans at early stages of the justice system. Provides outreach activities to prevent Veteran homelessness	First Name Middle Name Last Name Suffix Name SSN Date of Birth Gender Prisoner/Defendant ID Number Cell Location Facility/Court Name Facility/Court Zip Code Facility/Court State Parole Date	Secure electronic file transfer via HTTPS)/ (SSL)
/Healthcare for Reentry Veterans (HCRV) Program Provides outreach activities to prevent Veteran homelessness. HCRV is designed to address community re-entry needs of incarcerated Veterans.	First Name Middle Name Last Name Suffix Name SSN Date of Birth Gender Prisoner/Defendant ID Number Cell Location Facility/Court Name Facility/Court Zip Code Facility/Court State Parole Date Release or Hearing Date	Secure electronic file transfer via HTTPS)/ (SSL)
VA Office of Information Security/Office of Information Technology (OIT)	First Name Middle Name Last Name Suffix Name SSN Date of Birth Gender Prisoner/Defendant ID Number Cell Location Facility/Court Name Facility/Court Zip Code	Simple Object Access Protocol (SOAP) web service a messaging protocol that allows programs that run on disparate operating systems

Identify and list the names of any VA program offices, other VA organizations or IT systems <u>within</u> VA with which information is shared	Specifically list the Data Elements	Method of Transmission
	Facility/Court State Parole Date Release or Hearing Date	(such as Windows and Linux) to communicate using HTTPS.

4.2 <u>PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure</u>

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:

<u>Privacy Risk:</u>
There is a risk that data transferred in the VRSS may be shared with unauthorized individuals or that authorized personnel may share it with unauthorized individuals. The data may be disclosed to individuals who do not require access elevating the risk of the information being misused or improperly disclosed.

<u>Mitigation:</u>
Access control procedures mitigate the chance of unauthorized users. Authorized users are required to sign the National Rules of Behavior (or Contractor Rules of Behavior) as part of annual Privacy and Security Awareness training. The annual training provides guidance on the handling of VA sensitive information and describes the penalties associated for non-compliance and misuse.

The minimum security requirements for VRSS high impact system cover 17 security-related areas with regard to protecting the confidentiality, integrity, and availability of VA information systems and the information processed, stored, and transmitted by those systems. The security related areas include: access control; awareness and training; audit and accountability; certification, accreditation, and security assessments; configuration management; contingency planning; identification and authentication; incident response; maintenance; media protection; physical and environmental protection; planning; personnel security; risk assessment; systems and services acquisition; system and communications protection; and system and information integrity.

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?

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

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.

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

Identify and list the names of any program offices, contractor-supported IT systems, and any other organization or IT system <u>outside</u> the VA with which information is shared	**Specifically list the Data Elements Shared/Received**	**Type of Connection**	**Agreement Type (Can be more than one)**
N/A			

5.2 <u>PRIVACY IMPACT ASSESSMENT: External sharing and disclosure</u>

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 minimal limited risk that external sharing of data from the VRSS system may be misused.

Mitigation: No VA sensitive data is shared externally. Only an Inmate ID or Facility/Court ID and Facility/Court Location are returned to the correctional facilities/court systems (CF/CS). Access Control Procedures are in place to ensure that only authorized users have access to information.

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.

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.

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.

The information VRSS receives is collected by the correctional facilities/court systems then transmitted to the VA. The VA does not have the opportunity to notify the individuals before

collection. The Department of Veterans Affairs does provide public notice that the system does exist. This notice is provided in 2 ways:

1. The System of Record Notice (SORN) 121VA10- National Patient Databases-VA. This SORN can be found online at https://www.govinfo.gov/content/pkg/FR-2023-04-12/pdf/2023-07638.pdf.

2. This Privacy Impact Assessment (PIA) also serves as notice of the VRSS system.

As required by the eGovernment Act of 2002, Pub.L. 107–347 §208(b)(1)(B)(iii), the Department of Veterans Affairs "after completion of the [PIA] under clause (ii), make the privacy impact assessment publicly available through the website of the agency, publication in the Federal Register, or other means."

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.

VRSS data is collected by the correctional facilities/court systems then transmitted to the VA. The collecting institution would decide if the individual has the right to decline to provide information.

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.

VRSS data is collected by the correctional facilities/court systems then transmitted to the VA. The collecting institution would decide if the individual has the right to consent to particular uses of the information.

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:
There is minimal risk to the Department of Veterans Affairs that an individual within a correctional facility/court system has been notified of the collection of his/her personal information. There is a risk that members of the public may not know that the VRSS system exists within the Department of Veterans Affairs.

Mitigation:
The collecting institution would decide if the individual has the right to receive notice of the collection of his/her personal information. The VA mitigates the risk of public knowledge of the VRSS system by providing the public with two forms of notice that the system exists, as discussed in detail in question 6.1, including the PIA and a System of Record Notice.

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.

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.***

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).

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.

Individuals wishing to obtain more information from the VRSS system data should contact VA as directed in the System of Record Notice (SORN) 121VA10 "National Patient Databases-VA" found online at https://www.govinfo.gov/content/pkg/FR-2023-04-12/pdf/2023-07638.pdf. The SORN states:

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 or write or visit the VA facility location where they normally receive their care. A request for access to records must contain the requester's full name, address and 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.

Officials maintaining this system of records: Director, National Data Systems, Austin Information Technology Center, 1615 Woodward Street, Austin, Texas 78772. Telephone number 512–326–6780 (this is not a toll-free number).

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.

Individuals wishing to obtain more information about access, redress and record correction of VRSS system data should contact VA as directed in the System of Record Notice (SORN) 121VA10 "National Patient Databases-VA" found online at https://www.govinfo.gov/content/pkg/FR-2023-04-12/pdf/2023-07638.pdf.

Individuals seeking to contest or amend records in this system pertaining to them should contact the system manager in writing as indicated above. A request to contest or amend records must state clearly and concisely what record is being contested, the reasons for contesting it, and the proposed amendment to the record.

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.

The System of Record Notice (SORN) 121VA10 "National Patient Databases-VA" found online at https://www.govinfo.gov/content/pkg/FR-2023-04-12/pdf/2023-07638.pdf.

This Privacy Impact Assessment (PIA) also serves as notice of the how to request the correction of information.

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.

See 7.2 for formal redress processes.

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:
Access, redress, and correction policies and notification may not be sufficient to allow an individual the right to view or change their information. The individual may become frustrated with the results

of their attempt.

Mitigation:

By publishing this PIA and the applicable SORN, the VA makes the public aware of the VRSS system. Furthermore, this document and the SORN provide the point of contact for members of the public who have questions or concerns about this application/system: individuals may write or call the Director of National Data Systems (19F4), Austin Automation Center, 1615 Woodward Street, Austin, Texas 78772, or call the VA Austin Automation Center Help Desk and ask to speak with the VHA Director of National Data Systems at 512–326–6780

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.

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

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.

Per VA Directive and Handbook 6330, every 5 years the Office of Information Technology (OIT) develops, disseminates, and reviews/updates a formal, documented policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; along with formal, documented procedures to facilitate the implementation of the access control policy and associated controls.
OIT documents and monitors individual information system security training activities including basic security awareness training and specific information system security training. This documentation and monitoring is performed through the use of the Talent Management System (TMS).
Access to VRSS is granted by submitting a VA Form 9957 Access Request Form, containing several layers of approvals. The form must include the appropriate functional task codes relating to level of access that the user will require to perform his/her duties. Program staff, grant system access after verification of approval.

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 contract employee access is verified through the Contracting Officer's Representative (COR) and other VA supervisory/administrative personnel before access is granted to any VA system. Contractor access is reviewed annually at a minimum. The contractors who provide support to the system are required to complete annual VA Privacy and Information Security and Rules of behavior training via the VA Talent Management System (TMS). All contractors are vetted using the VA background investigation process and must obtain the appropriate level background investigation for their role. Contractors with systems administrative access are required to complete additional role-based training prior to gaining system administrator access. Generally, contracts are reviewed at the start of the initiation phase of acquisitions and again during procurement of option years by the Contracting Officer, Information Security Officer, Privacy Officer, COR, Procurement Requestor/Program Manager and any other stakeholders required for approval of the acquisition. Contracts generally have an average duration of 1-3 years and may have option years stipulated in the original contract.

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.

Personnel that will be accessing information systems 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 VA Privacy and Security Awareness training which all personnel must complete via the VA's Talent Management System (TMS). After the user's initial acceptance of the Rules, the user must re-affirm their acceptance annually as part of the privacy and security awareness training. Acceptance is obtained via electronic acknowledgment and is tracked through the TMS system.

All users with access to VA sensitive information or information system must complete VA Privacy and Security Awareness Rules of Behavior Training (TMS#10176) initially and annually thereafter. Additionally, if users will be accessing protected health information (PHI) data VA HIPAA Privacy training (TMS#10203) is required initially and annually thereafter.

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:* 1/26/2023
3. *The Authorization Status:* Approved
4. *The Authorization Date:* 1/6/2023
5. *The Authorization Termination Date:* 4/13/2023
6. *The Risk Review Completion Date:* 4/11/2023
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.***

Please provide response here

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.

N/A

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.*

N/A

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.

N/A

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.

N/A

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).

N/A

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**

ID	Privacy Controls
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
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.

Phillip Cauthers 255139

Digitally signed by Phillip Cauthers 255139
Date: 2023.06.01 09:30:28 -07'00'

Privacy Officer, Phillip Cauthers

JAMES B. ALDEN 201589

Digitally signed by JAMES B. ALDEN 201589
Date: 2023.06.01 16:10:21 -04'00'

Information System Security Officer, James Alden

Temperance M. Leister 3514567

Digitally signed by Temperance M. Leister 3514567
Date: 2023.06.01 14:55:32 -05'00'

Information System Owner, Temperance Leister

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).

System of Record Notice (SORN) 121VA10 "National Patient Databases-VA" can be found online at https://www.govinfo.gov/content/pkg/FR-2023-04-12/pdf/2023-07638.pdf.

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