Privacy Impact Assessment for the VA IT System called:

Salesforce: Quality Management System (QMS)

Office of Business Integration (OBI)
Veterans Benefits Administration

Date PIA submitted for review:
November 17, 2021

System Contacts:

<table>
<thead>
<tr>
<th>Role</th>
<th>Name</th>
<th>E-mail</th>
<th>Phone Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy Officer</td>
<td>Rita Grewal</td>
<td><a href="mailto:Rita.Grewal@va.gov">Rita.Grewal@va.gov</a></td>
<td>(202) 632-7861</td>
</tr>
<tr>
<td>Information System Security Officer (ISSO)</td>
<td>James Boring</td>
<td><a href="mailto:James.Boring@va.gov">James.Boring@va.gov</a></td>
<td>215-842-2000 x4613</td>
</tr>
<tr>
<td>Information System Owner</td>
<td>Michael Domanski</td>
<td><a href="mailto:Michael.Domanski@va.gov">Michael.Domanski@va.gov</a></td>
<td>727-595-7291</td>
</tr>
</tbody>
</table>
Abstract

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

The Quality Management System (QMS) consolidates quality reviews on Veterans Benefits Administration (VBA) claims in a single system. QMS is an effort to modernize the quality process and process improvement using the data obtained from the system. QMS provides a one stop shop for VBA quality reporting and analysis, reduces the response time for completing quality reviews, eliminates local variances in the quality process, reduces the work effort required to complete and manage quality reviews, and provides comprehensive quality reporting at the local and national level.

QMS performs and manages all quality reviews, including new and special reviews, for VBA Compensation Services, P&F (Pension and Fiduciary), Office of Administrative Review (OAR), Education Service (EDU), Office of Field Operations (OFO), Veteran Readiness & Employment Service (VR&E), Office of Transition and Economic Development (OTED), Office of Human Capital Services (HCS), and Office of Performance Analysis & Integrity (PA&I) Lines of Businesses. These reviews are performed on Veteran claims; therefore, the names collected in QMS are the claimant, Veterans and VA employee names performing the reviews.

QMS is built to interface and integrate with Enterprise Data Warehouse (EDW) to minimize data entry and to update EDW with the results of the quality reviews.

Employee types’ production records are captured automatically by other case management and production platforms utilized to complete their work (VSRs/RVSRs production records are captured in Veterans Benefits Management System (VBMS) and the data is stored outside of Salesforce with the Office of Performance Analysis and Integrity (PA&I). This system services nationwide and not a regional system.

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:

- The IT system name and the name of the program office that owns the IT system.
- The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission.
- Indicate the ownership or control of the IT system or project.
- The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.
- A general description of the information in the IT system and the purpose for collecting this information.
- Any information sharing conducted by the IT system. A general description of the modules and subsystems, where relevant, and their functions.
• 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.
• A citation of the legal authority to operate the IT system.
• Whether the completion of this PIA will result in circumstances that require changes to business processes
• Whether the completion of this PIA could potentially result in technology changes
• 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 Quality Management System (QMS) consolidates quality reviews on Veterans Benefits Administration (VBA) claims in a single system. QMS is an effort to modernize the quality process and process improvement using the data obtained from the system. QMS provides a one stop shop for VBA quality reporting and analysis, reduces the response time for completing quality reviews, eliminates local variances in the quality process, reduces the work effort required to complete and manage quality reviews, and provides comprehensive quality reporting at the local and national level.

QMS performs and manages all quality reviews, including new and special reviews, for VBA Compensation Services, P&F (Pension and Fiduciary), Office of Administrative Review (OAR), Education Service (EDU), Office of Field Operations (OFO), Veteran Readiness & Employment Service (VR&E), Office of Transition and Economic Development (OTED), Office of Human Capital Services (HCS), and Office of Performance Analysis & Integrity (PA&I) Lines of Businesses. These reviews are performed on Veteran claims; therefore, the names collected in QMS are the claimant, Veterans and VA employees’ names performing the reviews.

QMS is built to interface and integrate with Enterprise Data Warehouse (EDW) to minimize data entry and to update EDW with the results of the quality reviews.

Employee types’ production records are captured automatically by other case management and production platforms utilized to complete their work (VSRs/RVSRs production records are captured in VBMS and the data is stored outside of Salesforce with the Office of Performance Analysis and Integrity or PA&I). This system services nationwide and not a regional system.

To gain access to QMS users must use Single Sign On (SSO) service using a Personal Identification Verification (PIV) card and associated credentials.

QMS is covered by the Salesforce Authority to operate (ATO). There are no expected changes to the business process or technology based on this PIA.

The SORN, “VA Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records - VA” 58VA21/22/28 covers the use of PII in QMS module. The system does use cloud technology.

Ownership rights to PII data should be covered in the Salesforce contract. Per NIST 800-144, it is understood that the organization (VA) is ultimately accountable for security and privacy of data held by Salesforce on our behalf.
The magnitude of harm if PII was disclosed would have a negative impact on both the Cloud Service Provider (CSP) and VA. While there is limited data in the system through the Production component, that data could be used to negatively impact individuals’ credit, jobs, and other areas sensitive information can be used inappropriately. This could leave the CSP and VA open to litigation.

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 Account Information
☐ Health Insurance Beneficiary Numbers
☐ Certificate/License numbers
☐ Vehicle License Plate Number
☐ Internet Protocol (IP) Address Numbers
☐ Current Medications
☐ Previous Medical Records
☐ Race/Ethnicity
☐ Tax Identification Number
☐ Medical Record Number
☐ Gender
☐ Integration Control Number (ICN)
☐ Military History/Service Connection
☐ Next of Kin
☐ Other Unique Identifying Information (list below)
PII Mapped to Components

< Salesforce Quality Management System (QMS) > consists of <0> key components. Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by <QMS> 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.

<table>
<thead>
<tr>
<th>Database Name of the information system collecting/storing PII</th>
<th>Does this system collect PII? (Yes/No)</th>
<th>Does this system store PII? (Yes/No)</th>
<th>Type of PII (SSN, DOB, etc.)</th>
<th>Reason for Collection/Storage of PII</th>
<th>Safeguards</th>
</tr>
</thead>
<tbody>
<tr>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
</tr>
</tbody>
</table>

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

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?

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 1.3 indicate why the system is using this source of data.

If the system creates information (for example, a score, analysis, or report), list the system as a source of information.
This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.
Salesforce QMS utilizes Enterprise Data Warehouse (EDW) data maintained by Office of Performance Analysis and Integrity (PA&I) through an automatic file load from PA&I to salesforce module via MuleSoft Script.

1.3 How is the information collected?

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 technology used in the storage or transmission of information in identifiable form?

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.
This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

The information is collected via integrations with other VA systems to validate claimant entitlement, usage of entitlement and manage their benefits as per the CFR and public law. There exists a randomized report that utilizes Workforce and Time Reporting System (WATRS) maintained by Office of Field Operations, of completed claim information maintained by PA&I.

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

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.

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.
This question is related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.

The system is checked for accuracy against VBMS which holds the claims records to be reviewed and the WATRS system which holds the employee records regarding the work completed. The information is collated and provided by PA&I Enterprise Data Warehouse. The information is collected each time the data is pulled from the system.
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 5 U.S.C. 5514.

SORN (58VA21/22/28)

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.

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:**
Due to the highly sensitive nature of the data, there is a risk that, if the data were accessed by an unauthorized individual or otherwise breached; serious personal, professional, or financial harm may result for the individuals affected. Data breach may have at the network level.

**Mitigation:**
QMS adheres to the information security requirements instituted by the VA Office of Information Technology (OIT).

- All employees with access to claimant information are required to complete the VA Privacy and Information Security Awareness training and Rules of Behavior annually.
- Role based permissions will govern what participant information the data users will be able to access. The roles will be reviewed on a regular basis to ensure that appropriate information is shared with appropriate users.
- Multilevel security products from leading security vendors and proven security practices ensure network security. To prevent malicious attacks through unmonitored ports, external firewalls allow only https traffic on ports 80 and 443, along with Internet Control Message Protocol (ICMP) traffic.
- Switches ensure that the network complies with the Request for Comment (RFC) 1918 standard, and address translation technologies further enhance network security.
- IDS sensors protect all network segments. Internal software systems are protected by two-factor authentication, along with the extensive use of technology that controls point of entry.

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.*

QMS collects data of the Veterans listed below
Veteran First and Last Name: used to identify the Veteran and associate with the work completed.
Claimant Name: used to identify the dependent of the Veteran and associate with the work completed.
Social Security Number (SSN): when utilized as the file number assists in identifying the claims and benefits claims processed.
File Number: used to identify the claims and benefits program enrolled by the Veterans/dependents.

VA Employees data collected by the QMS tool are:
First and Last Name: used to identify who complete the claims processing work to quality review specified positions and employees on their work.

2.2 What types of tools are used to analyze data and what type of data may be produced?
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.

This question is related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information

The data created is related to the review of the processing of claims, and not newly created information directly related to the Veteran or claimant. The data is used for statistical analysis of the accuracy of the work being completed and is sanitized once a review of the claim work is completed.

2.3 How is the information in the system secured?
   2.3a What measures are in place to protect data in transit and at rest?

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

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

This question is related to security and privacy controls SC-9, Transmission Confidentiality, and SC-28, Protection of Information at Rest

QMS is accessed via a secured webpage utilizing SSO technology. QMS is housed in a vendor-owned AWS GovCloud, which is FedRAMP-certified and has security controls in place for safeguarding the data stored there.

Access to the PII is described by the System of Records Notice (SORN) for the QMS application can be found on-line at https://www.oprm.va.gov/privacy/systems_of_records.aspx 58VA21/22/28

Additional protection provided for SSN via Salesforce Shield Protect, which provides FIPS 140-2 certified encryption.

Following is the SORN number and data:
58VA21/22/28; Name: Compensation, Pension, Education, and Rehabilitation Records-VA.
The SORN defines the information collected from veterans, use of the information, and how the information is accessed and stored. The information collected is used for determining a veteran’s benefits, such as compensation or education.

QMS is implemented with the required security and privacy controls for Federal information systems and organizations according to NIST SP 800-53 and VA Handbook 6500, Risk Management Framework for VA Information Systems. Per the approval of the Assistant Secretary for information Technology, employees such as QRTs who are completing reviews have each undergone extensive background checks and has taken the required annual privacy training, as well as signed off on Rules of Behavior document.

Access to the QMS system is requested by the employee’s supervisor and approved by the system owner, through DTC. All users will be required to authenticate to the system with a PIV card and will only have permissions to perform their assigned function. Based upon that function, each user will only have access to information on those participants which are assigned to them by their manager. The system will perform extensive logging to detail all actions taken by a user. Some of these actions are (but not limited to):
1) Logon / Logoff
2) Create Data
3) Update Data
4) Delete Data

The QMS Privacy Officer, Information System Security Officer, and Information System Owner will be responsible for maintaining all safeguards put in place to protect PII and other sensitive information.

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information. 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?

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.
QMS is accessed via a secured webpage utilizing SSO technology. QMS is housed in a vendor-owned AWS GovCloud, which is FedRAMP-certified and has security controls in place for safeguarding the data stored there.

Access to the PII is described by the System of Records Notice (SORN) for the QMS application can be found on-line at https://www.oprm.va.gov/privacy/systems_of_records.aspx 58VA21/22/28

Following is the SORN number and data:
58VA21/22/28; Name: Compensation, Pension, Education, and Rehabilitation Records-VA.
The SORN defines the information collected from veterans, use of the information, and how the information is accessed and stored. The information collected is used for determining a veteran’s benefits, such as compensation or education.

QMS is implemented with the required security and privacy controls for Federal information systems and organizations according to NIST SP 800-53 and VA Handbook 6500, Risk Management Framework for VA Information Systems. Per the approval of the Assistant Secretary for information Technology, employees such as QRTs who are completing reviews have each undergone extensive background checks and has taken the required annual privacy training, as well as signed off on Rules of Behavior document.

Access to the QMS system is requested by the employee’s supervisor and approved by the system owner, through DTC. All users will be required to authenticate to the system with a PIV card and will only have permissions to perform their assigned function. Based upon that function, each user will only have access to information on those participants which are assigned to them by their manager. The system will perform extensive logging to detail all actions taken by a user. Some of these actions are (but not limited to):
1) Logon / Logoff
2) Create Data
3) Update Data
4) Delete Data

The QMS Privacy Officer, Information System Security Officer, and Information System Owner will be responsible for maintaining all safeguards put in place to protect PII and other sensitive information.

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

QMS collects the following information from Veterans and dependents:

- File Number
- Veteran SSN
- Claimant SSN
- Claimant Name
- Veteran Name.

QMS collects information the name from VA Employees completing work.

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. If the system is using cloud technology, will it be following the NARA approved retention length and schedule?

The VA records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented.

This question is related to privacy control DM-2, Data Retention and Disposal.

Records management within the Department of Veterans Affairs is governed by VA Directive 6300, Records and Information Management with specific records management procedures documented in VA Handbook 6300.1. At this time, all data collected and maintained by the QMS shall be kept and/or disposed of in accordance with the VA Records Control Schedule VB-1 Section II January 31, 2014.

The document can be located at the following URL: https://www.benefits.va.gov/WARMS/21guides.asp

3.3 Has the retention schedule been approved by the VA records office and the National Archives and Records Administration (NARA)? If so please indicate the name of the records retention schedule.

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.
This question is related to privacy control DM-2, Data Retention and Disposal.

QMS complies with all VA retention and disposal procedures specified in VA Handbook 6300 and VA Directive 6300. Records contained in the CMS instance will be retained as long as the information is needed in accordance with VA Records Control Schedule VB-1 Section II (January 31, 2014). Specific retention periods can be located in the VB-1 document at the following URL: https://www.benefits.va.gov/WARMS/21guides.asp

3.4 What are the procedures for the elimination of SPI?

Explain how records are destroyed or eliminated at the end of the 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

All claims’ files folders for Compensation and Pension claims are electronically imaged and uploaded into the VBMS eFolder. Once a file is electronically imaged and established by VA as the official record, its paper contents (with the exception of documents that are on hold due to pending litigation, and service treatment records and other documents that are the property of DoD), are reclassified as duplicate—non record keeping—copies of the official record, and will be destroyed in accordance with Records Control Schedule VB–1, Part 1 Section XIII, Item 13–052.100 as authorized by NARA.

All paper documentation that is not the property of VA (e.g., DoD-owned documentation) is currently stored by VA after scanning, pending a policy determination as to its final disposition. All documentation being held pursuant to active litigation is held in its native format during the pendency of the litigation. All VBMS eFolders are stored on a secure VA server, pending permanent transfer to NARA where they will be maintained as historical records. Prior to destruction of any paper source documentation reclassified as duplicate copies, VA engages in a comprehensive and multi-layered quality control and validation program to ensure material that has been electronically imaged is completely and accurately uploaded into the VBMS eFolder. To guarantee the integrity and completeness of the record, VA engages in industry-best practices, using state-of-the-art equipment, random sampling, independent audit, and 100% VA review throughout the claims adjudication process. Historically, VA’s success rate in ensuring the accuracy and completeness of the electronic record routinely and consistently exceeds 99%. Furthermore, no paper document is ever destroyed while any related claim or appeal for VA benefits is still pending. VA waits 3 years after the final adjudication of any claim or appeal before destroying the paper duplicate copies that have been scanned into the VBMS eFolder. As noted, the electronic image of the paper document is retained indefinitely as a permanent record either by VA or NARA. Decisions to destroy VR&E paper counseling records are to be made in accordance with Records Control Schedule (RCS), RCS VB–1, Part I, Field in Section VII, dated January 31, 2014.
Automated storage media containing temporary working information are retained until a claim is decided, and then destroyed. All other automated storage media are retained and disposed of in accordance with disposition authorization approved by NARA. Education file folders in paper are retained at the servicing Regional Processing Office. Education paper folders may be destroyed in accordance with the times set forth in the VBA Records Management, Records Control Schedule VB–1, Part 1, Section VII, as authorized by NARA. Employee productivity records are maintained for two years after which they are destroyed by shredding or burning. File information for CAIVRS is provided to HUD by VA on magnetic tape. After information from the tapes has been read into the computer the tapes are returned to VA for updating. HUD does not keep separate copies of the tapes.

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. Have policies and procedures been developed to minimize the use of PII for testing, training, and research? This question is related to privacy control DM-3, Minimization of PII Used in Testing, Training and Research

QMS only uses test data (no real PII) for testing the system. VA Handbook 6500 mandates that systems under development should not process “live data” or do any real processing in which true business decisions will be based. Test data that is de-identified should be used to test systems and develop systems that have not yet undergone security A&A. Furthermore, systems that are in development (pilot, proof-of-concept, or prototype) should not be attached to VA networks without first being assessed and authorized. Additionally, VA wide Directive 6511 describes the responsibilities, requirements, and procedures for eliminating PII or information exempt from release under FOIA from presentations that may be seen by non-VA parties. This directive includes guidance for conducting privacy reviews of presentations, and the criteria for when presenters must self-certify that their presentations are devoid of PII or information exempt from release under FOIA.

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.

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:**
As described herein, support systems retain information until that work in progress is completed and data is committed to master systems and records. The master systems retain data on a permanent basis (beyond the actual death of the claimant). If a master system is to be deactivated, critical information is migrated to the new system and the old system along with associated data is archived according to the application disposition worksheet. As such, SPI, PII or PHI may be held for long after the original record was required to be disposed. This extension of retention periods increases the risk that SPI may be breached or otherwise put at risk.

**Mitigation:**
Redaction of some information is required by law and protects the privacy interest of any individual who may have SPI, PII, or PHI which may appear in the data and files collected. Automated storage media containing temporary working information are retained until a claim is decided, and then destroyed. All other automated storage media are retained and disposed of in accordance with disposition authorization approved by NARA. The VA procedures for eliminating data are available from the VA Records Control Schedule VB-1 (January 31, 2014). The document can be located at the following URL:
https://www.benefits.va.gov/WARMS/21guides.asp

**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

<table>
<thead>
<tr>
<th>List the Program Office or IT System information is shared/received with</th>
<th>List the purpose of the information being shared/received with the specified program office or IT system</th>
<th>List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system</th>
<th>Describe the method of transmittal</th>
</tr>
</thead>
</table>
| Enterprise Data Warehouse | The system receives information from VBMS, WATRS, and QMS | Veterans or Dependents:  
- File Number  
- Veteran SSN  
- Claimant SSN  
- Claimant Name  
- Veteran Name  
VA Employees Names | The data is received by an automatic file load from PA&I to Salesforce module via MuleSoft Script. |

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

Follow the format below:

Privacy Risk:
There is a risk that QMS data may be shared with unauthorized individual(s), or that authorized users may share it with other unauthorized individuals. The risk might include end users who do not log out of the QMS when away from their computers.

Mitigation:
The VA requires single sign-on (SSO) or two-factor authentication (2FA) in order to access QMS. The following security control families are applicable (in addition to all NIST applicable RMF families):

- Audit and Accountability
- Awareness Training
- Security Assessment and Authorization
- Incident Response Personnel Security
- Identification and Authentication

The QMS personnel authenticate by using PIV/passwords before accessing claimant’s information. All personnel with access to claimant’s information are required to complete the VA Privacy and Information Security Awareness training and Rules of Behavior annually. In addition, the following will be used to provide additional risk mitigation:

- Role-Based Access Control (RBAC) permissions for all users
- Contractor users supporting the system take all required VA 6500-specified training for their role
- Role-Based privileged user training specific to the user’s role (i.e. A system administrator must be aware of certain functions that could threaten the system’s functionality/security posture)
- QMS adheres to all information security requirements instituted by the VA Office of Information Technology (OIT)
- Information is shared in accordance with the Privacy Act, HIPAA, FOIA and VA policy.

The tool will have a definable “time-out” setting which will automatically log the user out after a period of inactivity.

### 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 3.11 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

<table>
<thead>
<tr>
<th>List External Program Office or IT System information is shared/received with</th>
<th>List the purpose of information being shared / received / transmitted with the specified program office or IT system</th>
<th>List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program or IT system</th>
<th>List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)</th>
<th>List the method of transmission and the measures in place to secure data</th>
</tr>
</thead>
<tbody>
<tr>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
</tr>
</tbody>
</table>

QMS information is not shared with external organizations.

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:** N/A
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 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?

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. If notice was provided in the Federal Register, provide the citation.

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.

QMS does not directly collect information from individuals. Specifically, any information that relates to collection from an individual is collected and maintained in an alternate system which is covered under SORN Access to the PII is described by the System of Records Notice (SORN) for the QMS application can be found on-line at https://www.oprm.va.gov/privacy/systems_of_records.aspx?58VA21/22/28

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 information reporting can be declined in general however, declining to provide information could affect entitlement to benefits. This statement is provided on any forms submitted by the individual under privacy notice.
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

Any information provided is given with general consent for use 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.

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 a risk that claimants and employees may not understand the kind of information needed to determine entitlement to programs or to ensure the correct benefits and services are provided according to the information gathered about the claimant which is also utilized to review the internal processing of claims work.

**Mitigation:**
The VA mitigates this risk by providing the public with two forms of notice that the system exists, as discussed in detail in question 6.1, including this Privacy Impact Assessment and the associated System of Record Notice (SORN).

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?
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.

This question is related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.

Any information utilized in QMS is minimal and request for information as it relates to this information. However, if the individual wants quality information FOIA procedures must be followed as outlined in 38 CFR Part 1.

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.

Generally, the information collected would not require correction on the part of the claimant however, the employee may request correction and the procedures followed are outlined in the quality review process for each respective entity in the QMS system in M21-4.

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.

Employees are notified as part of training and guidance published internal to VA in M21-4.

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. This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Example: Some projects allow users to directly access and correct/update their information online. This helps ensure data accuracy.

Not applicable for this tool, described above.

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.

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:
There is a risk that individuals may seek to access or redress records in the QMS and 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 unique status of applications and evidence files. Furthermore, this document and the SORN provide the point of contact (POC) for members of the public who have questions or concerns about applications and evidence files. All access and redress issues are utilizing the same POC. Prior written consent or a power of attorney authorizing access is required before VA will allow the representative or attorney
to have access to the claimant’s automated claims records. Contact information is listed by facility in the SORN.

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?

*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.*

*This question is related to privacy control AR-7, Privacy-Enhanced System Design and Development.*

Contractor support teams possess privileged users responsible for maintaining the system on behalf of the VA. VA role-based security training is required for all privileged users of VA systems. Single sign-on utilizing VA PIV cards and/or Citrix VPN (over contractor laptops and unsecure networks) will be required. Typical privileged users of QMS include:

- Systems Engineer(s) - Privileged Access
- System Administrator(s) – Privileged Access
- Information System Security Engineers (Continuous Monitoring) - Auditor

The contractor shall follow all VA rules and regulations regarding information security to prevent disclosure of sensitive information to unauthorized individuals or organizations. The contractor may have access to Protected Health Information (PHI) and Electronic Protected Health Information (EPHI) that is subject to protection under the regulations issued by the Department of Health and Human Services, as mandated by the Health Insurance Portability and Accountability Act of 1996 (HIPAA); 45 CFR Parts 160 and 164, Subparts A and E, the Standards for Privacy of Individually Identifiable Health Information (“Privacy Rule”); and 45 CFR Parts 160 and 164, Subparts A and C, the Security Standard (“Security Rule”). Pursuant to the Privacy and Security Rules, the contractor must agree in writing to certain mandatory provisions regarding the use and disclosure of PHI and EPHI.

User roles identify the information and applications a user can access. To receive access to the system, another user of with appropriate permissions must sponsor them. The sponsor will
describe which applications the user needs to access, the user’s role, and any security caveats that apply to the user. These roles will be governed by permission sets that allow field level control of the information and data.

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 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 security awareness training. Acceptance is obtained via electronic acknowledgment and is tracked through the TMS system. System administrators are required to complete additional role-based training. All administrative users undergo mandated annual training, including privacy and HIPAA focused training and VA privacy and information security awareness training.

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

If Yes, provide:

1. The Security Plan Status,
2. The Security Plan Status Date,
3. The Authorization Status,
4. The Authorization Date,
5. The Authorization Termination Date,
6. The Risk Review Completion Date,
7. The FIPS 199 classification of the system (LOW/MODERATE/HIGH).

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

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

The Security Plan Status: Approved
The Security Plan Status Date: 02/24/2021
The Authorization Status: ATO
The Authorization Date: 03/18/2021
The Authorization Termination Date: 12/17/2023
The Risk Review Completion Date: 03/12/2021
The FIPS 199 classification of the system – Moderate

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).

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.

QMS utilizes a Cloud Service Provider (CSP). Salesforce Subscription Licenses, Maintenance and Support, Contract Number: NNG15SD27B. This software utilizes the PaaS Service of Salesforce Gov 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)

This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.


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.

No ancillary data is collected.

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.

Yes, the principle is described in the contract.

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).

QMS does not utilize RPA.
## Section 10. References

### Summary of Privacy Controls by Family

<table>
<thead>
<tr>
<th>ID</th>
<th>Privacy Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>AP</td>
<td><strong>Authority and Purpose</strong></td>
</tr>
<tr>
<td>AP-1</td>
<td>Authority to Collect</td>
</tr>
<tr>
<td>AP-2</td>
<td>Purpose Specification</td>
</tr>
<tr>
<td>AR</td>
<td><strong>Accountability, Audit, and Risk Management</strong></td>
</tr>
<tr>
<td>AR-1</td>
<td>Governance and Privacy Program</td>
</tr>
<tr>
<td>AR-2</td>
<td>Privacy Impact and Risk Assessment</td>
</tr>
<tr>
<td>AR-3</td>
<td>Privacy Requirements for Contractors and Service Providers</td>
</tr>
<tr>
<td>AR-4</td>
<td>Privacy Monitoring and Auditing</td>
</tr>
<tr>
<td>AR-5</td>
<td>Privacy Awareness and Training</td>
</tr>
<tr>
<td>AR-7</td>
<td>Privacy-Enhanced System Design and Development</td>
</tr>
<tr>
<td>AR-8</td>
<td>Accounting of Disclosures</td>
</tr>
<tr>
<td>DI</td>
<td><strong>Data Quality and Integrity</strong></td>
</tr>
<tr>
<td>DI-1</td>
<td>Data Quality</td>
</tr>
<tr>
<td>DI-2</td>
<td>Data Integrity and Data Integrity Board</td>
</tr>
<tr>
<td>DM</td>
<td><strong>Data Minimization and Retention</strong></td>
</tr>
<tr>
<td>DM-1</td>
<td>Minimization of Personally Identifiable Information</td>
</tr>
<tr>
<td>DM-2</td>
<td>Data Retention and Disposal</td>
</tr>
<tr>
<td>DM-3</td>
<td>Minimization of PII Used in Testing, Training, and Research</td>
</tr>
<tr>
<td>IP</td>
<td><strong>Individual Participation and Redress</strong></td>
</tr>
<tr>
<td>IP-1</td>
<td>Consent</td>
</tr>
<tr>
<td>IP-2</td>
<td>Individual Access</td>
</tr>
<tr>
<td>IP-3</td>
<td>Redress</td>
</tr>
<tr>
<td>IP-4</td>
<td>Complaint Management</td>
</tr>
<tr>
<td>SE</td>
<td><strong>Security</strong></td>
</tr>
<tr>
<td>SE-1</td>
<td>Inventory of Personally Identifiable Information</td>
</tr>
<tr>
<td>SE-2</td>
<td>Privacy Incident Response</td>
</tr>
<tr>
<td>TR</td>
<td><strong>Transparency</strong></td>
</tr>
<tr>
<td>TR-1</td>
<td>Privacy Notice</td>
</tr>
<tr>
<td>TR-2</td>
<td>System of Records Notices and Privacy Act Statements</td>
</tr>
<tr>
<td>TR-3</td>
<td>Dissemination of Privacy Program Information</td>
</tr>
<tr>
<td>UL</td>
<td><strong>Use Limitation</strong></td>
</tr>
<tr>
<td>ID</td>
<td>Privacy Controls</td>
</tr>
<tr>
<td>------</td>
<td>--------------------------------------</td>
</tr>
<tr>
<td>UL-1</td>
<td>Internal Use</td>
</tr>
<tr>
<td>UL-2</td>
<td>Information Sharing with Third Parties</td>
</tr>
</tbody>
</table>
Signature of Responsible Officials

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

RITA K GREWAL
114938
Digitally signed by RITA K GREWAL 114938
Date: 2021.12.20 11:22:05 -05'00'  
Privacy Officer, Rita Grewal

James C. Boring
149438
Digitally signed by James C. Boring 149438
Date: 2022.01.03 15:44:52 -05'00'  
Information Security Systems Officer, James Boring

Michael S. Domanski 326889
Digitally signed by Michael S. Domanski 326889
Date: 2022.01.12 11:02:13 -05'00'  
System Owner, Michael Domanski
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).

Privacy, Policies, And Legal Information | Veterans Affairs