Privacy Impact Assessment for the VA IT System called:

Veterans Claim Intake Processing Source Material Tracking System (VCIP SMTS)

Veterans Claim Intake Program

Date PIA submitted for review:

7/27/2020

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>Annmarie Braggs</td>
<td><a href="mailto:Annmarie.Braggs@va.gov">Annmarie.Braggs@va.gov</a></td>
<td>202.461.9292</td>
</tr>
<tr>
<td>Information System Security Officer (ISSO)</td>
<td>Richard Alomar-Loubriel</td>
<td><a href="mailto:Richard.Alomar-Loubriel@va.gov">Richard.Alomar-Loubriel@va.gov</a></td>
<td>787.696.4091</td>
</tr>
<tr>
<td>Information System Owner</td>
<td>Derek Herbert</td>
<td><a href="mailto:Derek.Herbert@va.gov">Derek.Herbert@va.gov</a></td>
<td>202.461.9606</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 VCIP Source Material Tracking System (VCIP SMTS) allows users to manage, locate, track, update and report on Paper Mail artifacts undergoing Conversion (digitization, routing and upload to VBMS or DMHS) in support of the Veterans Benefit Administrations (VBA) eligibility determination processes. The system is a managed service platform hosted by the vendor on GovCloud and used by the vendor Paper Mail handlers and support staff as well as by VA personnel and their approved representatives.

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.
- The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.
- If your system is a regional GSS, VistA, or LAN, include a list of the hospitals/medical centers, or other regional offices that fall under your system. Additionally, what region is the system under?
- A general description of the information in the IT system.
- 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?
- Does the system use cloud technology? 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.
- Does a contract with Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII?
• **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 is the magnitude of harm if privacy related data is disclosed, intentionally or unintentionally?** Would the reputation of the CSP or its customers (VA) be affected?

The system name Veterans Claim Intake Program Source Material Tracking System (VCIP SMTS) is owned by the Veterans Claims Intake Processing organization of the Veterans Benefit Administration (VBA). VCIP SMTS allows users to manage, locate, track, update and report on Paper Mail artifacts undergoing digital conversion routing and upload to designated Veterans Affairs Administration (VA) downstream systems in support of the VBA’s eligibility determination processes. The system is developed, maintained and hosted by vendor GovernmentCIO (GCIO) and used by Paper Mail handlers and support staff and VA personnel and their approved representatives. To fulfill its source material tracking objective, VCIP SMTS collects one or more of the following fields: Name, Address, Date of Birth, Document Control Number, Participate number and Unique Identifier.

VCIP SMTS will receive and store primary the VA unique identifier file number for tracking mail related to a Veteran. Note that for some Veterans the file number provided matches their Social Security numbers. VCIP SMTS is able to track all data within the system by using the unique identifier file number (all data is stored in an encrypted data repository). Data is managed in accordance with the Health Insurance Portability and Accountability Act (HIPAA) requirements for tracking PII/PHI information within the Source Mailing Tracking System. Legal Authority: “Title 38, U.S.C. Chapter 3, Section 210 (c) (1), Title 38 U.S.C. 7301, 5 U.S.C. 552a.and Executive order 9397.”

VCIP SMTS will be hosted in AWS FedRAMP compliant (Non-VAEC) Gov Cloud and inherits associated FedRAMP security controls. External access to the system is controlled via (and in compliance with) VA’s designated single sign on (SSO) interface, which facilitates two factor authentications. Internal factory users of the system access via local two factor authentication within the factory firewalls.

---

**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 Account Information
- Health Insurance Beneficiary Numbers
- Account 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
- Other Unique Identifying Number (list below)

Document control number participate number and VA file numbers.

PII Mapping of Components

VCIP Source Material Tracking System (VCIP SMTS) consists of one key component. The component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by VCIP Source Material Tracking System (VCIP SMTS) and the reasons for the collection of the PII are in the table below.

PII Mapped to Components

<table>
<thead>
<tr>
<th>Components of the information system (servers) 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>VCIP SMTS</td>
<td>Yes</td>
<td>Yes</td>
<td>Name, Address, Date of Birth, Document</td>
<td>VCIP SMTS will be able to track all data within the</td>
<td>Personal Identity Verification (PIV)</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.

In support of VCIP SMTS primary mission of making Veteran’s information gathering and processing more efficient and timelier, Team GCIO receives source materials directly from the Post Office, mail couriers (e.g. United Parcel Service), VBA Regional Offices (Ros), Veterans Service Organizations (VSOs) and third parties providing evidence in support of a claim.

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.
Paper Mail artifacts come into the vendor factory from the Post Office, United Parcel Service and other mail couriers designated and engaged by the VA. The factory intakes that mail and the VCIP SMTS is provided tracking information from the factory’s internal data systems via a secure Virtual Private Network (VPN) connection as mail goes through the factory conversion process.

1.4 What is the purpose of the information being collected, used, disseminated, created, or maintained?

*Include a statement of why the particular SPI is collected, maintained, used, or disseminated in the system is necessary to the program’s or agency’s mission. Merely stating the general purpose of the system without explaining why this particular type of information should be collected and stored is not an adequate response to this question.*

*If the system collects, uses, disseminates, or maintains publicly available or commercial data, include a discussion of why commercial data is relevant and necessary to the system’s purpose. This question is related to privacy control AP-2, Purpose Specification.*

Information is collected in SMTS to track and report on the intake, processing, rescanning and delivery of artifacts submitted to Team GCIO under the terms of the Paper Mail Conversion and Management Services (PMCMS) contract.

1.5 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.*

SMTS has built-in field validation and Team GCIO’s Quality Team performs regular sampling audits of the system by reviewing reports. The VA also has independent auditors contracted and their personnel are stationed onsite at the Team GCIO processing factory. The six personnel perform regular and ongoing
audits of all materials processed by our factory systems and provide regular reports to the VA Contracting Officer Representative (COR) and Program Manager (PM) for the Paper Mail Conversion and Management Services (PMCMS) contract. Finally, VCIP Administrators are the administrators of the VCIP SMTS application and review the system’s accuracy on an ongoing basis via canned reports and ad hoc queries.

1.6 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

The authorization for operation of VCIP is VA Contract No. VA118-16-D-1003 Purchase Order 36C10B20N1003008, with Federal authorization to collect information under: “Title 38, U.S.C. Chapter 3, Section 210 (c) (1), Title 38 U.S.C. 7301, 5 U.S.C. 552a, and Executive order 9397.”

1.7 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:** There is risk that the information may be accessed by unauthorized individual

**Mitigation:** PIV access is utilized. VCIP SMTS uses the latest encryption and integrity algorithms for all point of communication to ensure the privacy of the PII data (such as AES256, SHA1, SHA2-256, ikev1 and ikev2), and is, under this contract, enhancing security with the implementation of the VA’s Single Sign On capability which enforces multifactor authentication.

**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.*

The VA’s VBA organization will use the SMTS system to track materials that have been provided to Team GCIO for conversion and rescans so that they can better understand where veteran records are in the conversion process. Reports in VCIP SMTS allow VCIP SMTS users, supervisors and VCIP Administrators to what elements of the veteran record have been processed and delivered to downstream VA systems.

**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 stored in VCIP SMTS is limited to the information necessary to track artifacts that have been processed under the PMCMS contract (important note: the content of the artifacts is not stored in VCIP SMTS).

The VCIP SMTS users can track artifacts that are converted from analog to digital, structured data and they are able to view reports indicating the time taken to process provided artifacts from the point of intake to the point of delivery to downstream VA applications. VCIP tooling is oriented to determine the efficiency of the Team GCIO factory processes for conversion

2.3 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.

All data collected, processed, transmitted and stored in VCIP SMTS is treated as Sensitive. All persons associated with operating the system receive training (initial, annual refresher and ad hoc) on Privacy Act, Health Insurance Portability and Accountability Act (HIPAA), system data security and VA Rules of Behavior (ROB). The VCIP SMTS access control system includes role-based access control (RBAC) based on the following:

- Multi-factor authentication for factory system operators
- SSO for VA employees, contractors and designated operators
- Basic User Access
- Quality Assurance Access
- Supervisor Access
- VCIP Administrator Access
System Administration Access

User requests are reviewed and approved by both supervisors and administrators in the User Account Management module of VCIP. All account management actions are logged. All access to and update of records is logged. The vendor team, VA Supervisors and VCIP Administrators are all responsible for reviewing access to and use of VCIP SMTS.

The vendor team runs regular scans required by the VA and the reports are both reviewed internally and provided to government oversight teams for review. POAMs are executed to track and resolve findings in compliance with the PMCMS contract.

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?

Name, Address, Date of Birth, Document control number participate number, Unique identifier file numbers that sometime is used as the social security numbers and VA file numbers

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

Seven years unless otherwise specified by the VBA.

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.

The system data retention schedule is specified and compliant with the base contract, and any changes specified in the Interconnection Security Agreement (ISA)/Memorandum of Understanding (MOU). Information contained in the system is restricted to minimum required to meet system objectives.

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.

No Veteran’s records are destroyed by the VCIP SMTS system. Factory systems data is flushed every 90 days on a rolling basis as de-prepared mail packets are assembled and shipped to long term storage (LTS) per contract requirements. In the event the Government directed Team GCIO to destroy paper mail artifacts, the artifacts would be destroyed in accordance with the requirements of NIST SP 800-88, Media Sanitization.”

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.

Not applicable no live data for PII/PHI will be used for testing, training and research.

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:** The information received from Data Dimension will be retained for the required time for the Privacy Act.

**Mitigation:** Veteran PI/SPI is encrypted during transmission and storage. Data is only retained in compliance with the PMCMS contract requirements and is purged programmatically when retention period is reached. Only authorized and trained personnel can access VCIP SMTS.

**Section 4. Internal Sharing/Receiving/Transmitting and Disclosure**

The following questions are intended to define the scope of information sharing/receiving/transmitting within VA. NOTE: Question 5 on Privacy Threshold Analysis should be used to answer this question.

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?

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 data element types such as PII/PHI that are shared/received with the Program Office or IT system</th>
<th>Describe the method of transmittal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Dimension</td>
<td>To facilitate the tracking, monitoring and reporting of Veteran paper mail that is or has been converted to digitized searchable files under the PMCMS contract.</td>
<td>Name, Address, Date of Birth, Document Control Number, Participant number and Unique Identifier numbers/Social Security numbers.</td>
<td>Site to Site (S2S) VPN, TCP, SHA 256</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Users of VCIP access the secure system via VA SSO functionality with VA issued Personal Identity Verification (PIV) cards, which enforces multifactor authentication and also ensure that background checks and required training is completed and sustained.</td>
</tr>
</tbody>
</table>

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:** Users of VCIP SMTS could share their screens or reports that are exported from the web application

**Mitigation:** All VA employees are required to complete training for managing PI/PII/SPI in the course of performing theirs jobs. The VCIP System also logs access to the application and additionally logs updates and deletes and report downloads to allow VCIP Administrators to monitor access and use of VCIP SMTS.
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: This question is #7 in the Privacy Threshold Analysis.

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 data element types such as PII/PHI that are shared/received 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>IAM</td>
<td>Request authority to proceed PIV confirmation through SAML</td>
<td>No PII/PHI</td>
<td>Notice is provided by VBA-Compensation, Pension, Education, and Vocational Rehab and Employment Records. VBA Systems of Records Notice (SORN) # 58VA21, 58VA22, and 58VA28. <a href="https://www.oprm.va.gov/docs/CurrentSORNList_7_16_20.pdf">https://www.oprm.va.gov/docs/CurrentSORNList_7_16_20.pdf</a></td>
<td>Application Program Interface (API)</td>
</tr>
</tbody>
</table>

If specific measures have been taken to meet the requirements of OMB Memoranda M-06-15 and M-06-16, note them here.

Completed the ATA SSOi Application v6

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 No information is being shared VCIP SMTS will request authority to proceed PIV confirmation through SAML transmitted through the Application Program Interface (API)

There is a small risk that information maybe shared with an external organization or agency.

Mitigation: N/A Safeguards are implemented to ensure data is not shared with unauthorized organizations, including employee security and privacy training, and required reporting of suspicious activity. Personal Identification Verification (PIV) cards is required to gain access. All measures that are utilized for the system. Interconnection Security Agreement (ISA) and Memorandum of Understanding (MOU) are kept current and monitored closely to ensure protection of 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 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.

Notice is provided by VBA-Compensation, Pension, Education, and Vocational Rehab and Employment Records. VBA Systems of Records Notice (SORN) # 58VA21, 58VA22, and 58VA28
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.

Veterans have the right to refuse to disclose their SSNs to VBA. The individual shall not be denied any right, benefit, or privilege provided by law because of refusal to disclose to VBA an SSN (please refer to the 38 Code of Federal Regulations CFR 1.575(a)).

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.

All requests must be in writing and adequately describe the specific information the individual believes to be inaccurate, incomplete, irrelevant, or untimely and the reason for this belief. The written request needs to be mailed or delivered to the VBA address outlined within the SORN.

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:** N/A VCIP SMTS does not deal with the intake of the physical package itself but deals with the status of the package during the digitization and archiving process

**Mitigation:** N/A

---

**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.*

Veterans may request access to Privacy Act records maintained by requesting a copy in writing. All requests to review must be received by direct mail, fax, in person, or by mail referral from another agency or VA office. All requests for access must be delivered to and reviewed by the System Manager for the concerned VBA system of records, the facility Privacy Officer, or their designee. Each request must be date stamped and reviewed to determine whether the request for access should be granted.

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.

Veterans have the right to amend their records by submitting their request in writing. The request must be in writing and adequately describe the specific information the individual believes to be inaccurate, incomplete, irrelevant, or untimely and the reason for this belief. The written request needs to be mailed or delivered to the VBA that maintains the record. A request for amendment of information contained in a system of records must be delivered to the System Manager or designee for the concerned VBA system of records, and the facility Privacy Officer or designee, and needs to be date stamped; and filed appropriately. In reviewing requests to amend or correct records, the System Manager must be guided by the criteria set forth in VA regulation 38 CFR 1.579.

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.

No direct feedback from Veterans. All information collect was given by Veteran. The Veterans provide their information directly either by mail, or a form they will submit their information in a paper form and will be digital conversion routing and upload to designated Veterans Affairs Administration (VA) downstream systems in support of the VBA's eligibility determination processes. This process is done prior to VCIP SMTS receiving the digitalized record. SMTS will not correct any information received digitally, so VCIP SMTS would not be aware if the information received is being inaccurate 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. 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 ensures data accuracy.
Formal redress is provided. All information correction must be taken via the Amendment process.

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 the paper mail that is received and undergoes conversion under the PMCMS contract will enter provided information and that it will be incorrect and there is the risk that the provided data is correct but incorrectly transposed into VCIP SMTS.

Mitigation: The data entered into the source tracking system is a subset of the data processed for delivery to VA downstream systems. When the affected source material is entered into the Veterans Benefits Management System (VBMS) and associated with a Veterans case(s), the team will be able to correct incorrect data.

Additionally, the Team GCIO factory has extensive controls and processes in place to track and audit the processing of all Veteran paper mail processed under the PMCMS contract. The embedded document outlines our processes.
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.*

Access control is maintained in accordance with FIPS Publication 199 *Moderate* information system control standards. Team GCIO follows the Principle of Least Privilege when approving access to any system and/or data. System users and administrators are given only the minimum access necessary to perform their function(s). Standard minimum access profiles are maintained via roles defined for the VCIP SMTS application. Role-based access requests and revocations are processed within the application. The Team GCIO System Administrator verifies requests are made from valid VA accounts and then the requests are processed by a VBA Station Supervisor and final approval is granted by the VCIP Administrators.

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 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.*

VCIP SMTS is a contractor-furnished and maintained system. At the end of the PMCMS contract the system shut down and access terminated.
For VA employees and the designees (which may include contractors), multifactor authentication leveraging SSO with a PIV card is enforced. PIV cards are terminated at contract end.

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 PHI are trained to handle it appropriately. This question is related to privacy control AR-5, Privacy Awareness and Training.

All persons associated with VCIP SMTS development, operation, and maintenance receive initial entry, annual refresher, and ad hoc training on privacy, including the Privacy Act, HIPAA, system and data security, and the VA Rules of Behavior (ROB)

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

If Yes, provide:

1. The date the Authority to Operate (ATO) was granted,
2. Whether it was a full ATO or ATO with Conditions,
3. The amount of time the ATO was granted for, and
4. 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 enhanced implementation of VCIP SMTS with SSO enabled, improved performance and enhanced reporting capabilities is targeted to be release to production August 9, 2020. The FIPS 199 classification for VCIP SMTS is a Moderate system.
## Section 9. 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>Authority and Purpose</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>Accountability, Audit, and Risk Management</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>Data Quality and Integrity</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>Data Minimization and Retention</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>Individual Participation and Redress</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>Security</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>Transparency</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>Use Limitation</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>
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).

Notice is provided by VBA-Compensation, Pension, Education, and Vocational Rehab and Employment Records. VBA Systems of Records Notice (SORN) # 58VA21, 58VA22, and 58VA28

https://www.oprm.va.gov/docs/CurrentSORNList_7_16_20.pdf

Signature of Responsible Officials

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

Annmarie E. Braggs 1412218

PO, Annmarie Braggs

Date: 2020.12.02 18:56:24 -05'00'

RICHARD ALOMAR-LOUBRIEL 139039

Information Security Systems Officer, Richard Alomar-Loubriel

Date: 2020.12.03 11:36:15 -05'00'

DEREK L. HERBERT 312060

System Owner, Derek Herbert

Date: 2020.12.02 14:53:58 -05'00'