



Privacy Impact Assessment for the VA IT System called:

Veterans Claims Intake Program Conversion Services Assessing (VCIP-CS)

Veterans Benefits Administration (VBA)

Office of Business Integration (OBI)

U:VA:1062 / CAM ID# AP0021113

Date PIA submitted for review:

08/06/2026

System Contacts:

	Name	E-mail	Phone Number
Privacy Officer	Marvis Harvey	Marvis.Harvey@va.gov	(202)-461-8401
Information System Security Officer (ISSO)	Jose Diaz	Jose.Diaz4@va.gov	(312)-980-9606
Information System Owner	John Clark	John.Clark7@va.gov	(708)-483-5575

Abstract

The abstract provides the simplest explanation for “what does the system do for VA?”.

Veterans Claim Intake Program Conversion Services (VCIP-CS) converts benefits application source materials to searchable pdf format. The system generates the images, indices and extracted metadata from the source materials and uploads same to Veterans Benefits Administration (VBA) via Veterans Benefits Administration – Veterans Benefit Management System (VBMS) to achieve deliver, a term that refers to the upload of data to the upload service and confirmation that the transaction was successful. It also has the Source Materials Tracking System (SMTS) which aids the tracking of materials from storage (origin) to process facilities, through the conversion and return to long term storage. Additionally, the Centralized Benefits Communication Management (CBCM), also a component of Veterans Claim Intake Program Conversion Services (VCIP-CS) allows Regional Offices to send mail to veterans through a centralized service. (CBCM) conducts document retrieval, batch communication receipt and document preparation/packaging services for outbound communications to veterans. Unified Claims Accelerated Platform (UCAP) The Unified Claims Acceleration Platform (UCAP) is an enterprise framework for intelligent claims processing, integrating workflow automation and secure data exchange to help support VA’s goal of accelerating benefits decision with improved accuracy, lowering backlogs.

Overview

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

1 General Description

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

Veterans Claim Intake Program Conversion Service (VCIP-CS) takes scanned images of Veterans benefits-related records and uploads them to the Veterans Benefits Management System. It also tracks the source material from receipt at the processing site through scanning, uploading, and de-preparation for long- term storage. The system is hosted on AWS GovCloud. The system also has a component that manages printing and mailing letters to Veterans. The users include Veterans Benefits Administration (VBA) internal personnel as well as GDIT personnel with specific responsibilities and role-based access. The UCAP component accelerates claims processing and improves accuracy resulting in backlog reduction

- B. Who is the owner or has control of the IT system or project? If the system has an eMASS entry, ensure this information matches with the eMASS entry.*

Vendor owned (GDIT) and VA Controlled Veterans Benefits Administration (VBA).

2. Information Collection and Sharing

- C. *Indicate the expected number of individuals whose information is stored in the system and include a brief description of the typical client or affected individual?*

About 2.5 million veterans.

Check if Applicable	Demographic of individuals
☒	Veterans or Dependents
☐	VA Employees
☐	Clinical Trainees
☐	VA Contractors
☐	Members of the Public/Individuals
☐	Volunteers

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

The source materials could contain PII/PHI including Social Security Number, Date of birth, mailing address. These are not collected directly from veterans but are extracted from source materials and benefits applications documents.

- E. *What information sharing is conducted by the IT system? A general description of the modules and components, where relevant, and their functions.*

Veterans Claim Intake Program Conversion Services (VCIP-CS) component applications (File Conversion Services (FCS), Centralized Benefits Communication Management (CBCM) and Unified Claims Accelerated Platform have a site-to-site connection with Veterans Benefits Administration – Veterans Benefit Management System (VBMS) for the purpose of transmitting data to Veterans Benefits Administration (VBA) through (VBMS)

- F. *Are the modules/subsystems only applicable if information is shared?*

Yes.

- G. *Is the system operated in more than one site to include primary and secondary 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?*

The system components are hosted on AWS GovCloud instance. Users access the system from VBA Regional Offices. The associated database is encrypted at rest and in transit. Users, (role-based) are also required to complete VA clearance prior to having access. The system is only accessed from facilities with approved Physical and Environmental (PE) controls in place.

3. Legal Authority and System of Record Notices (SORN)

H. What is the citation of the legal authority?

The issuance of the Performance Work Statement (PWS) and the GDIT contract with VA conveyed the legal authority to operate Veterans Claim Intake Program Conversion Services (VCIP-CS). The legal authority is supported by; Privacy Act of 1974, 5 U.S.C. § 552a • Confidential Nature of Claims, 38 U.S.C § 5701 • HIPAA Privacy Rule, 45 C.F.R. Part 164 • Confidentiality of Certain Medical Records, 38 U.S.C. § 7332 • Confidentiality of healthcare Quality Assurance Review Records, 38 U.S.C. § 5705 • Freedom of Information Act, 5 U.S.C. § 552

I. What is the SORN?

SORN Information; https://www.oprm.va.gov/privacy/systems_of_records.aspx
<https://www.govinfo.gov/content/pkg/FR-2025-09-15/pdf/2025-17709.pdf>

58VA21/22/28 Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA

J. If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval.

The SORN does not require any changes.

4. System Changes

K. Will the business processes change due to the information collection and sharing?

☐ Yes

☒ No

if yes, <<ADD ANSWER HERE>>

I. Will the technology changes impact information collection and sharing?

☐ Yes

☒ No

if yes, <<ADD ANSWER HERE>>

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 Information 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 | ☐ Financial Information | Number (ICN) |
| ☒ Full Social Security Number | ☐ Health Insurance Beneficiary Numbers | ☒ Military History/Service Connection |
| ☐ Partial Social Security Number | ☐ Account Numbers | ☐ Next of Kin |
| ☒ Date of Birth | ☐ Certificate/License Numbers ¹ | ☒ Date of Death |
| ☐ Mother's Maiden Name | ☐ Vehicle License Plate Number | ☐ Business Email Address |
| ☒ Personal Mailing Address | ☐ Internet Protocol (IP) Address Numbers | ☐ Electronic Data Interchange Personal Identifier (EDIPI) |
| ☒ Personal Phone Number(s) | ☐ Medications | ☐ Other Data Elements (List Below) |
| ☐ Personal Fax Number | ☐ Medical Records | |
| ☒ Personal Email Address | ☐ Race/Ethnicity | |
| ☒ Emergency Contact Information (Name, Phone Number, etc. of a Different Individual) | ☐ Tax Identification Number | |
| | ☐ Medical Record Number | |
| | ☒ Sex | |
| | ☐ Integrated Control | |

Other PII/PHI data elements: None.

1.2 List the sources of the information in the system

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

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

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

The source materials are shipped from VA storage locations to the processing sites. The information is extracted from scanned images and documents (source materials). The system does not directly collect PII/PHI from individuals.

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

The system's function is to scan hard copy benefits application documents and store those images in searchable PDF, as well as extract metadata from the documents. This is to make the documents/data readily available for Veterans Benefits Administration (VBA) benefits processing.

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

File Conversion Services (FCS), a component Veterans Claim Intake Program Conversion Services (VCIP-CS) can be listed as the source of information for the reports generated for VBA leadership. The report includes metrics of performance, statistics, and metadata from scanned source materials.

1.3 Methods of information collection

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

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

Information is contained and derived from source materials. Information is not collected directly from individuals.

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

This is not applicable. An OMB control number or agency form number is not required.

1.4 Information checks for accuracy, and how often will it be checked.

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

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

The information in the scanned images cannot be changed. The extracted information from the source materials goes through Quality Assurance and is parsed by the system for accuracy.

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

The system does not use a commercial aggregator to check for accuracy of information.

1.5 Identify the specific legal authorities, arrangements, and agreements that 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 issuance of the Performance Work Statement (PWS) and the GDIT contract with VA conveyed the legal authority to operate Veterans Claim Intake Program Conversion Services (VCIP-CS) The legal authority is supported by; Privacy Act of 1974, 5 U.S.C. § 552a • Confidential Nature of Claims, 38 U.S.C § 5701 • HIPAA Privacy Rule, 45 C.F.R. Part 164 • Confidentiality of Certain Medical Records, 38 U.S.C. § 7332 • Confidentiality of healthcare Quality Assurance Review Records, 38 U.S.C. § 5705 • Freedom of Information Act, 5 U.S.C. § 552.

SORN Information; https://www.oprm.va.gov/privacy/systems_of_records.aspx

<https://www.govinfo.gov/content/pkg/FR-2025-09-15/pdf/2025-17709.pdf>

58VA21/22/28 Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA

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: *The collection ties with the purpose of the underlying mission of the organization and its enabling authority.*

Principle of Minimization: The information is directly relevant and necessary to accomplish the specific purposes of the program.

Principle of Individual Participation: The program, to the extent possible and practical, collects information directly from the individual.

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

Follow the format below when entering your risk assessment:

Privacy Risk:

The major existent privacy risk with the information and data associated with the program/system is data loss and inadvertent disclosure.

Mitigation:

PHI and PII are contained in the source material, File Conversion Services (FCS) does not use PHI or PII as metadata. File Conversion Services (FCS) limits the access to source materials and converted data by automating the conversion process, using FIPS 140-3 compliant encryption for data at rest and data in transit. FIPS 140-3 protocols are used to transmit data as outlined in the system description. All File Conversion Services (FCS) personnel require a minimum NACI background investigation. Based on role and level of access a SAC may be required. Personnel security requirements for SAC are outlined in the MOU with Veterans Benefits Administration (VBA).

Section 2. Uses of the Information

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

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

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

PII/PHI Data Element	Internal Use	External Use
Name	Used for veteran Identification purposes.	Used for identifying veterans in workflow creation.
Social Security Number	Used to identify and associate a veteran to their record.	Used for identifying veterans in workflow creation.

Date of Birth	Used to identify veteran's age.	Used for identifying veterans in workflow creation.
Personal Mailing Address	Used to send mail to the veteran.	Contained in files in workflow.
Sex	Used to identify the sex of the veteran.	Used for identifying veterans in workflow creation.
Personal Phone	Used to identify a veteran.	Used for identifying veterans in workflow creation.
Emergency Contact	Might be contained in scanned or processed source material	Contained in files in workflow.
Military History	Might be contained in scanned or processed source material	Contained in files in workflow.
Date of Death	Might be contained in scanned or processed source material	Contained in files in workflow.

2.2 Describe the types of tools used to analyze data and what type of data may be produced.

These questions are related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information.

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

File Conversion Services (FCS) as well as Centralized Benefits Communication Management (CBCM) and Unified Claim Accelerated Platform (UCAP) (components of Veterans Claim Intake Program Conversion Services (VCIP-CS) have capability to generate reports and performance analysis. Reports analysis and presentation are done using Tableau plugin. The system mostly aggregates the number of scanned images or source materials processed and keeps track of the processing timeline.

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

The system does not create or add any new information about an individual. However, for the purpose of searching and identifying individual records, the system creates a unique Records Management Number (RMN) for individuals. This number is used to search and identify an individual's record.

2.3 How the information in the system is secured.

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

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

File Conversion Services (FCS) limits the access to source materials and converted data by automating the conversion process, using FIPS 140-3 compliant encryption for data at rest and data in transit. FIPS 140-3 protocols are used to transmit data as outlined in the system description. All File Conversion Services (FCS) personnel require a minimum National Agency Check and Inquiry (NACI) background investigation. Based on role and level of access a Special Agreement Check (SAC) may be required. Personnel security requirements for SAC are outlined in the MOU with Veterans Benefits Administration (VBA).

2.3b If the system is collecting, processing, or retaining Social Security Numbers, are there additional protections in place to protect SSNs? (refer to PTA question 3.8).

While File Conversion Services (FCS) / Centralized Benefits Communication Management (CBCM) and UCAP do not directly collect SSN and other PII/PHI, there are measures in place to protect the sensitive information extracted from source materials. The data is encrypted at rest and in transit. Also, physical access to the processing area as well as source materials is strictly restricted to ONLY VA-cleared personnel (SAC) with approved business and functional need.

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

While File Conversion Services (FCS) / Centralized Benefits Communication Management (CBCM) do not directly collect SSN and other PII/PHI, there are measures in place to protect the sensitive information extracted from source materials. The data is encrypted at rest and in transit. Also, physical access to the processing area as well as source materials is strictly restricted to ONLY VA-cleared personnel (SAC) with approved business and functional need. This information is not shared with any entity other than Veterans Benefits Administration (VBA) through Veterans Benefits Administration – Veterans Benefit Management System (VBMS).

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information.

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

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

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

Principle of Use Limitation: *Is the use of information contained in the system relevant to the mission of the project?*

This question is related to privacy control AR-4, Privacy Monitoring and Auditing, AR-5, Privacy Awareness and Training, and SE-2, Privacy Incident response.

2.4a How is access to the PII determined?

Access to PII is determined based on Role/function. Role-Based Access Control (RBAC) is strictly implemented to ensure only persons with business need to know have access. Prior to provisioning access, personnel must complete requisite Information Security training and User Acceptable Policy. They must also complete SAC level clearance prior to getting access to work on materials containing PII.

2.4b Are criteria, procedures, controls, and responsibilities regarding access documented? How are the documented, i.e. Policy, SOP, other. And where is this documentation located?

Yes. There is record of all personnel on the project and the record identifies those who have completed the requirements for having access to sensitive information. There is also a continuous monitoring process to ensure the conditions for granting access is maintained.

2.4c Does access require manager approval?

Every access request requires manager approval.

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

This is in place and strictly monitored.

2.4e Who is responsible for assuring safeguards for the PII as identified in eMASS?

There is a Program Information Security Officer who works with project management team at the facilities to ensure the safeguards are put in place for PII to remain efficient. The Program/GDIT Information System Security PoC reports to the VA system Information System Security Officer (ISSO).

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

The system extracts and retains the following information for a period determined by Veterans Benefits Administration (VBA):

- Full name
- Date of Birth
- Social Security Number
- Personal Mailing Address
- Sex
- Personal mailing address
- Personal phone number

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 <https://www.archives.gov/records-mgmt/grs>? This question is related to privacy control DM-2, Data Retention and Disposal.

File Conversion Services (FCS) retains source materials, images, and image metadata for a period determined by Veterans Benefits Administration (VBA) (60 days for source materials) following confirmation of successful upload to Veterans Benefits Administration – Veterans Benefit Management System (VBMS). After successful upload, the images are archived in encrypted DB for the length of the project. File Conversion Services (FCS) shall store source materials onsite where document conversion occurred in conditions and security consistent to source material awaiting scanning. At the conclusion of processing, File Conversion Services (FCS) ship source materials to VA's Records Management Services vendor for storage awaiting disposition.

3.3 The retention schedule approved by the VA records office and the National Archives and Records Administration (NARA).

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

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

Yes.

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

The retention period and disposition are determined and effected by Veterans Benefits Administration (VBA). Per the program Performance Work Statement (PWS), data is retained in encrypted DB for the life of the contract. The operations data converted images and files are held in a

Relational Database for 90 days, after which the files are moved into a secure, encrypted S3 bucket and held for the length of the contract.

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

Explain how records are destroyed, eliminated, or transferred to NARA at the end of their mandatory retention period. Please give the details of the process. For example, are paper records shredded on site, or by a shredding company and accompanied by a certificate of destruction, etc.? This question is related to privacy control DM-2, Data Retention and Disposal.

File Conversion Services (FCS) limits the use for SPI to the converted documents as outlined in the specifications in PWS and the MOU with Veterans Benefits Administration (VBA). The system does not directly use SPI for processing the scanned images or documents. Files are mapped to unique Records Management Number (RMN) generated for the records. The (RMN) is also used for locating a record, eliminating the need to pull records with SSN or other PII. The system and associated database reside on Amazon AWS GovCloud. Records are transmitted to Veterans Benefits Administration (VBA) through Veterans Benefits Administration – Veterans Benefit Management System (VBMS) and the server decommissioned when no longer required.

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

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

File Conversion Services (FCS) does not use PII/PHI nor SPI for research, testing and training purposes. The environment, designed to have a production and preproduction environments uses dummy data for testing and training purposes. This is intended to preserve privacy and reduce potential risks associated with the unauthorized disclosure of the information.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

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

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

Principle of Minimization: The project retains only the information necessary for its purpose, additionally, the PII is retained only for as long as necessary and relevant to fulfill the specified purposes.

Principle of Data Quality and Integrity: The PIA should describe 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: Unauthorized or inadvertent disclosure of information.

Mitigation: Scanned images are stored in a database and encrypted both at rest, in transit and in process. The SPI management is in line with the PWS specifications as well as approved VA guidelines and the ISA MOU with Veterans Benefits Administration – Veterans Benefit Management System (VBMS). All personnel are trained in Sensitive information management procedure as well as complete related VA TMS training and User Acceptance Policy acknowledgement.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

PII Mapping of Components

4.1a Veterans Claim Intake Program Conversion Services (VCIP-CS) consists of three key components (servers/databases/instances/applications/software/application programming interfaces (API)). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by VCIP-CS and the reasons for the collection of the PII are in the table below.

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

Internal Components Table

Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards

Veterans Claim Intake Program Conversion Services (VCIP-CS)	Yes	Yes	Full names SSN Date of Birth Personal Mailing Address Sex	For VCIP-CS business purposes	Encrypted S2S connection
Centralized Benefits Communication Management (CBCM)	Yes	Yes	Full names SSN Date of Birth Personal Mailing Address Sex	For VCIP-CS business purposes	Encrypted S2S connection
Unified Claims Accelerated Platform (UCAP)	Yes	Yes	Full names SSN Date of Birth Personal Mailing Address Sex	For VCIP-CS business purposes	Encrypted S2S connection

4.1b List internal organizations information is shared/received/transmitted, the information shared/received/transmitted, and the purpose, and how the information is 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

IT system and/or Program office. Information is shared/received with	List the purpose of the information being shared /received with the specified program office or IT system	List PII/PHI data elements shared/received/transmitted.	Describe the method of transmittal
Veterans Benefits Administration – Veterans Benefit Management System (VBMS)	VA owns the data the system generates. Veterans Benefits Administration (VBA) retains the digitized data/images in (VBMS). The purpose is for the data/information to be used in making benefits applications decisions	Full names Date of Birth SSN Personal Mailing address Sex	Information/data is transmitted via a secure and encrypted Site to Site connection to (VBMS)
Data Access Services (DAS)	A part of Veterans Benefits Administration (VBA), data aids in making benefits applications processing decisions faster.	Full names Date of Birth SSN Personal Mailing address Sex	S3 to S3 Connection

4.2 **PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure**

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

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

Follow the format below:

Privacy Risk: Unauthorized or inadvertent disclosure of information.

Mitigation:

Scanned images are stored in a database and encrypted both at rest, in transit and in process using FIPS 140-3 compliant standard. Access to system is restricted to only approved FIPS 140- 3 devices. Authentication method is also set up to use personal identity verification (PIV) cards for (PIV)-issued personnel and multi factor authentication (MFA) for non-PIV users. The SPI management is in line with the PWS specifications as well as approved VA guidelines and the ISA MOU with Veterans Benefits Administration – Veterans Benefit Management System (VBMS). All personnel are trained on Sensitive information management procedure as well as complete related VA TMS training and User Acceptance Policy acknowledgement.

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 List the external organizations (outside VA) that information shared/received. and information shared/received, and the purpose, and how the information transmitted and what measures are taken to ensure it is secure.

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

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

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

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

Describe how the information is transmitted to entities external to VA and what security measures have been taken to protect it during transmission.

This question is related to privacy control UL-2, Information Sharing with Third Parties

<i>List IT System or External Program Office information is shared/received with</i>	<i>List the purpose of information being shared / received / transmitted</i>	<i>List the specific PII/PHI data elements that are processed (shared/received/transmitted)</i>	<i>List agreements such as: Contracts, MOU/ISA, BAA, SORN. etc. that permit external sharing (can be more than one)</i>	<i>List the method of transmission and the measures in place to secure data</i>
Pega	Data modeling to support UCAP component and creation User IDs	Name, Full Social Security Number, Date of Birth, Personal Mailing Address, Sex.	MOU/ISA	S3 to S3 Connection/API Gateway

5.2 **PRIVACY IMPACT ASSESSMENT: External sharing and disclosure**

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

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

Discuss whether access controls have been implemented and whether audit logs are regularly reviewed to ensure appropriate sharing outside of the Department. For example, is there a Memorandum of Understanding (MOU), contract, or agreement in place with outside agencies or foreign governments.

Discuss how the sharing of information outside of the Department is compatible with the stated purpose and use of the original collection.

This question is related to privacy control AR-2, Privacy Impact and Risk Assessment, AR-3, Privacy Requirements for Contractors and Service Providers, and AR-4, Privacy Monitoring and Auditing

Follow the format below:

Privacy Risk:

Inadvertent release or exposure of sensitive information during transmission to external systems.

Mitigation:

The transmission is done via secure API integration/calls. Role-based access control is also in place to ensure that only authorized personnel with functional and business need to know have access to the system and files.

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 The notice provided to the individual before collection of the information. Please provide a copy and/or screen shot of a web notice of the notice as an Appendix-A 6.1 on the last page of the document. (A notice may include a posted privacy policy, a Privacy Act notice on forms, notice given to individuals by the sources system, or a system of records notice published in the Federal Register.) If notice was not provided, explain why.

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

6.1a Provide the Privacy Notice provided to the public by this system or any source systems. Include a copy of the notice in Appendix A of the PIA, the Federal Register citation, or Privacy Statement from collection of information such as forms or surveys.

File Conversion Services (FCS) and Centralized Benefits Communication Management (CBCM) do not directly collect personal or personal health information nor SPI from individuals. However, as mentioned earlier, benefits application documents, which are the source materials being converted, extracted and transmitted to Veterans Benefits Administration (VBA) through Veterans Benefits Administration – Veterans Benefit Management System (VBMS) may contain PII and/or PHI. The requisite notice is provided by Veterans Benefits Administration (VBA), which is responsible for collecting information from individuals. The notice is contained in the SORN, <https://www.govinfo.gov/content/pkg/FR-2025-09-15/pdf/2025-17709.pdf>. The project PWS empowers the system to receive the source materials from the VA or the storage facilities.

6.1b If notice was not provided, explain why.

Notice is provided in SORN, 58VA21/22/28 Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA

<https://www.govinfo.gov/content/pkg/FR-2025-09-15/pdf/2025-17709.pdf>

6.1c Provide how the notice provided at the time of collection meets the purpose of use for this system.

File Conversion Services (FCS) and Centralized Benefits Communication Management (CBCM) does not directly collect personal or personal health information nor SPI from individuals.

However, as mentioned earlier, benefits application documents, which are the source materials being converted, extracted and transmitted to Veterans Benefits Administration (VBA) through Veterans Benefits Administration – Veterans Benefit Management System (VBMS) may contain PII and/or PHI. The requisite notice is provided by Veterans Benefits Administration (VBA), which is responsible for collected the information from individuals. The project PWS empowers the system to receive the source materials from the VA or the storage facilities.

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.

File Conversion Services (FCS), Unified Claim Accelerated Platform (UCAP) and Centralized Benefits Communication Management (CBCM) do not directly receive nor collect SPI from individuals. They are sent to Veterans Benefits Administration (VBA) directly. The discretion to either provide or decline to provide PII/PHI resides between the veteran and Veterans Benefits Administration (VBA).

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.

The component systems function is limited to document conversion and image data transfer, benefits related mail handling and tracking of source materials. There is no direct interaction or exchange with individuals or public. The right to consent to any use of information is determined by VA - Veterans Benefits Administration (VBA) and retains the responsibility to notify the individuals or information owners.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

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

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

Principle of Transparency: *This is referring to sufficient notice provided to the individual.*

Principle of Use Limitation: *The information used only for the purpose for which notice was provided either directly to the individual or through a public notice. The procedures in place must 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:

Likelihood of individuals not having comprehensive knowledge of how their information is going to be used, processed or stored.

Possible unauthorized access, use or inadvertent disclosure of personal information.

Mitigation:

The VA has provided a detailed SORN: <https://www.govinfo.gov/content/pkg/FR-2025-09-15/pdf/2025-17709.pdf> which provides adequate information and notice regarding personal information in the system.

The system does not directly collect personal information from veterans. The system only scans, converts and extracts information from source materials as well as receive, batch and print and send benefits related mails to veterans. The source materials, however, might contain personal information. The responsibility for notice issuance lies with Veterans Benefits Administration (VBA). The system does not make use of, nor share individuals' information for any purpose. A unique Records Management Number (RMN) is generated by the system and assigned to individual records for the purpose of searching for records.

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 The procedures that allow individuals to gain access to their information.

These questions are related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.

*7.1a Cite any procedures or regulations your program has in place that allow access to information. These procedures, at a minimum, should include the agency's FOIA/Privacy Act practices, but may also include additional access provisions. **For example, if your program has a customer satisfaction unit, that information, along with phone and email contact information, should be listed in this section in addition to the agency's procedures. See 5 CFR 294 and the VA FOIA Web page at [VA Public Access Link-Home \(efoia-host.com\)](https://efoia-host.com) to obtain information about FOIA points of contact and information about agency FOIA processes.***

File Conversion Services (FCS), Centralized Benefits Communication Management (CBCM) and Unified Claim Accelerated Platform (UCAP), all components of VCIP-CS system are subject to

FOIA/Privacy Act. Individual needing access to their information held or processed by the system would send a FOIA request via the VBA Regional Offices which triggers the release of the requestor's information to them, through VBA. Individuals' access to their information are directly channeled to Veterans Benefits Administration (VBA) systems.

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

The system is not exempted.

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

Individuals seeking access to their information contained in the system will route the request directly to Veterans Benefits Administration (VBA).

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.

File Conversion Services (FCS) and Centralized Benefits Communication Management (CBCM) does not collect veteran information, Source materials and Benefits mail often contain veteran information and are scanned or mailed as is/received. If there is need for individuals to correct their information, that request or process is managed by Veterans Benefits Administration (VBA).

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.

Since the Veterans Benefits Administration (VBA) collects veteran information, there will also be a means of notifying individuals of any need to make corrections in their information. This is outside the scope of the system.

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

Redress is the process by which an individual gains access to his or her records and seeks corrections or amendments to those records. Redress may be provided through the Privacy Act and

*Freedom of Information Act (FOIA), and also by other processes specific to a program, system, or group of systems. **Example: Some projects allow users to directly access and correct/update their information online. This helps ensure data accuracy.***

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

This is outside the scope of the system. Veterans Benefits Administration (VBA) would have a means of letting individuals/veterans correct or update their information.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

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

***Principle of Individual Participation:** The individual must be provided with the ability to find out whether a project maintains a record relating to them.*

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

***Principle of Individual Participation:** The mechanism by which an individual is able to prevent information about them obtained for one purpose from being used for other purposes without their knowledge.*

This question is related to privacy control IP-3, Redress.

Follow the format below:

Privacy Risk:

An individual/veteran's inability to access their information and/or make corrections to the information if it was incorrect.

Mitigation:

Individual seeking to make corrections or updates to their records submit such requests to VBA where the requests are reviewed and decided on. The correction to any records is made in the VBA's Veterans Benefits Management System (VBMS).

Section 8. Technical Access and Security

The following questions are intended to describe technical safeguards and security measures. (Work with your ISSO to complete this section).

8.1 The procedures in place to determine which users may access the system, must be documented.

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

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

Access to the File Conversion Services (FCS), Unified Claim Accelerated Platform (UCAP) and Centralized Benefits Communication Management (CBCM) is strictly role based on need to know. Access is granted to VA-cleared, with valid business or functional need to know. personal identity verification (PIV) issued personnel with role-based need access applications using (PIV) as means of authentication while non-PIV users access via multi factor authentication (MFA). In both cases, accounts are pre-provisioned on request and approval.

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

This is not applicable. Only VA users have access. The other users will be GDIT personnel cleared by VA to work on the program.

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

The system has Admin users, Super User Account, Test accounts with access to complete testing, and read-only account.

8.2. Contractor signed Non-Disclosure Agreement (NDA), Business Associate Agreement (BAA) etc. in place.

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.

8.2a Has a contractor confidentiality agreement, Business Associate Agreement (BAA), or a Non-Disclosure Agreement (NDA) been developed for contractors who work on the system?

There is a BAA, NDA and User acceptable policy in place.

8.2a. Will VA contractors have access to the system and the PII?

Yes, GDIT developers and admins including testers go through VA SAC clearance to be on the program. Other GDIT personnel on the project all have VA sponsored SAC clearance prior to getting access.

8.2b. What involvement will contractors have with the design and maintenance of the system?

File Conversion Services (FCS), Unified Claim Accelerated Platform (UCAP) and Centralized Benefits Communication Management (CBCM) is developed, owned and managed by GDIT, a VA contractor as a SaaS offering thus, system is GDIT-owned and VA-Controlled.

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.

Users are required to complete the VA Privacy and Information Security Awareness and Rules of Behavior training on VA TMS platform. There is also a GDIT provided recurrent training for system users.

8.4 The Authorization and Accreditation (A&A) completed for the system.

8.4a If completed, provide:

1. *The Security Plan Status: Approved*
2. *The System Security Plan Status Date: 05/06/2025*
3. *The Authorization Status: Authorized to Operate (ATO)*
4. *The Authorization Date: 05/16/2025*
5. *The Authorization Termination Date: 05/08/2028*
6. *The Risk Review Completion Date: 03/18/2025*
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH): Moderate*

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

*8.4b If not completed or In Process, provide your **Initial Operating Capability (IOC) date.***

ATO was granted for Veterans Claim Intake Program Conversion Services (VCIP-CS) on 05/08/2025

Section 9 – Technology Usage

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

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

If so, Does the system have a FedRAMP provisional or agency authorization? If the system does use cloud technology, but does not have FedRAMP authorization, explain how the Cloud Service Provider (CSP) solution was assessed and what FedRAMP documents and processes were used for the assessment in order to comply with VA Handbook 6517. Types of cloud models include: Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS),

Commercial off the Shelf (COTS), Desktop as a Service (DaaS), Mobile Backend as a Service (MBaaS), Information Technology Management as a Service (ITMAaaS). This question is related to privacy control UL-1, Information Sharing with Third Parties.

The system is cloud-based and a single-tenant SaaS model, hosted on AWS GovCloud.

9.2 Does the contract with the Hosting 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.

Per contract (VA 20-00081754) terms, VA has full ownership of all data relating to the system, both system and transactional data. The Cloud service provider is Amazon AWS GovCloud.

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.

All data generated during the system's operations is owned by VA

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.

VA works with GDIT to ensure requisite security controls are in place to secure, protect and preserve the privacy of information and data relating to the Veterans Claim Intake Program Conversion Services (VCIP-CS) system and components.

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).

The system does not utilize RPA.

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

Signature of Responsible Officials

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

MARVIS HARVEY Digitally signed by MARVIS HARVEY
Date: 2026.08.27 06:01:41 -05'00'

Privacy Officer, Marvis Harvey

JOSE DIAZ Digitally signed by JOSE DIAZ
Date: 2026.09.01 13:23:54 -05'00'

Information System Security Officer, Jose Diaz

JOHN CLARK Digitally signed by JOHN CLARK
Date: 2026.09.02 09:40:36 -05'00'

Information System Owner, John Clark

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; screen shot of a website collection privacy notice).

The notice is contained in the SORN, <https://www.govinfo.gov/content/pkg/FR-2025-09-15/pdf/2025-17709.pdf>

HELPFUL LINKS:

Records Control Schedule 10-1 (va.gov)

General Records Schedule

<https://www.archives.gov/records-mgmt/grs.html>

National Archives (Federal Records Management):

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

VA Publications:

<https://www.va.gov/vapubs/>