Privacy Impact Assessment for the VA IT System called:

# Salesforce: Office of Integrity and Compliance (OIC) Oversight and Accountability Reporting and Visualization Platform (OARVP) Compliance Inquiry Reporting & Tracking System (CIRTS) 2.0

## Office of Integrity and Compliance (OIC)

## Veterans Health Administration (VHA)

Date PIA submitted for review:

08/01/2022

System Contacts:

*System Contacts*

| | Name | E-mail | Phone Number |
|---|---|---|---|
| Privacy Officer | Phillip Cauthers | Phillip.cauthers@va.gov | 503-721-1037 |
| Information System Security Officer (ISSO) | James Boring | james.boring@va.gov | 215-842-2000, 4613 |
| Information System Owner | Michael Domanski | michael.domanski@va.gov | 727-595-7291 |

## Abstract

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

The Compliance Inquiry Reporting & Tracking System (CIRTS) 2.0 application is used by Compliance Officers at each VISN/VA Medical Center and by Program Compliance Officers to record and track the receipt and disposition of reports and/or concerns related to matters of the business integrity of VHA operations while investigating allegations of compliance violations or inquiries pertaining to compliance guidance. The purpose of the CIRTS 2.0 application is to establish a process to receive reports of suspected compliance violations and compliance inquiries, and to maintain a system to respond to such allegations and inquiries.

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

- *The IT system name and the name of the program office that owns the IT system.*
- *The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission.*
- *Indicate the ownership or control of the IT system or project.*
- *The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.*
- *A general description of the information in the IT system and the purpose for collecting this information.*
- *Any information sharing conducted by the IT system. A general description of the modules and subsystems, where relevant, and their functions.*
- *Whether the system is operated in more than one site, and if so, a description of how use of the system and PII is maintained consistently in all sites and if the same controls are used across sites.*
- *A citation of the legal authority to operate the IT system.*
- *Whether the completion of this PIA will result in circumstances that require changes to business processes*
- *Whether the completion of this PIA could potentially result in technology changes*
- *If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval? If the system is using cloud technology, does the SORN for the system cover cloud usage or storage?*

The Compliance Inquiry Reporting & Tracking System (CIRTS) 2.0 will be built on Salesforce.com, a cloud-based Software as a Service (SaaS) platform. This solution provides a comprehensive and integrated approach to caregiver record management by streamlining processes and improving reporting capability. The CIRTS application is used by Compliance Officers and Compliance Staff (approximately 200-300 users total) at each VA Medical Center, VISN and Program Office. The CIRTS 2.0 system is established to control the receipt and disposition of inquiries and allegations deemed to be under the oversight of Integrity and Compliance or received through the Compliance Helpline including but not limited to: Enrollment; Means Testing; Eligibility; Pre-certification and certification/utilization review; Standards pertaining to documentation, coding and billing; inquiries and remediation; Accounts receivable and payable; Information protection, record retention,

information for general compliance inquiries; Provider documentation supporting business processes; Overpayments; Questionable conduct on the part of managers, supervisors or employees as related to business processes; and any other matter relating to the business integrity of VHA operations.

Information in the CIRTS 2.0 system pertaining to allegations or inquiries will not routinely be shared with any other VA system or entity except when the result of triage actions within the CIRTS 2.0 application require a referral to another organization for action. VHA Office of Integrity and Compliance has the same responsibility and requirement that all VA employees must report instances of waste fraud and abuse that are discovered during investigations to the VA Office of the Inspector General (OIG). The System of Records governing CIRTS 2.0 is 106VA17 "Compliance Record, Response, and Resolution of Reports of Persons Allegedly Involved in Compliance Violations—VA", https://www.govinfo.gov/content/pkg/FR-2009-08-17/pdf/E9-19628.pdf. The legal authority to operate the IT system is Title 38 USC Section 501, Title 38 USC 7332, and 45 CFR Parts 160 and 164.

Information collection and data entry are performed by Compliance Officer and/or Compliance Staff at VHA facilities, VHA VISNs, VHA Program Offices and VHA Central Office. Only OIC Program Office personnel, Compliance Officers and approved Compliance Staff have access to enter data into the system. OIC Program Office personnel and Compliance Officers are the only ones that will collect information. Information collected may include: (1) Name; (2) DOB (3) phone number; (4) issue/claim; (5) location (facility, office, department); (6) date of service/issue/close out; (7) free text including resolution facility information; (8) investigation results, actions taken, notes, dates, evident and outcomes; (9) risk profile potential Information may be in prepopulated and structure fields for the use to form a narrative summary or synopsis, exhibits, or internal documentation and memoranda.

User accounts are created with specific privileges to the application. These accounts are controlled through credentials that are managed by the application. Access to computerized information in the database is restricted to authorized personnel on a need-to-know basis. User accounts are provisioned and governed by VA IT via Single-Sign-On (SSO) to the Salesforce platform. Computer system documentation will be maintained in a secure environment in the VHA Office of Integrity and Compliance, and in the Compliance Offices at the network and medical center locations with PIV card login authentication. Physical access to printouts and data terminals will be limited to authorized personnel in the Compliance Program. Access to physical file folders is restricted to authorized personnel on a need-to-know basis. Paper files are maintained in file cabinets or closets and are locked at all times and only unlocked for employee access. These files are under the control of the Compliance Officer or his/her designees. VHA buildings are protected from unauthorized access by a protective service, and visitors are authorized to enter the building with limited access to VHA office spaces.

## Section 1. Characterization of the Information

The following questions are intended to define the scope of the information requested and collected as well as the reasons for its collection as part of the program, IT system, or technology being developed.

**1.1 What information is collected, used, disseminated, created, or maintained in the system?**

*Identify and list all Sensitive Personal Information (SPI) that is collected and stored in the system, including Individually Identifiable Information (III), Individually Identifiable Health Information (IIHI), Protected Health Information (PHI), and Privacy- Protected Information. For additional information on these information types and definitions, please see VA Directives and Handbooks in the 6500 series (https://vaww.va.gov/vapubs/). If the system creates information (for example, a score, analysis, or report), list the information the system is responsible for creating.*

*If a requesting system receives information from another system, such as a response to a background check, describe what information is returned to the requesting system.*
*This question is related to privacy control AP-1, Authority to Collect, and AP-2, Purpose Specification.*

*The information selected below must match the information provided in question 2.1 as well as the data elements columns in 4.1 and 5.1.*

Please check any information listed below that your system collects, uses, disseminates, creates, or maintains. If additional SPI is collected, used, disseminated, created, or maintained, please list those in the text box below:

- ☒ Name
- ☐ Social Security Number
- ☒ Date of Birth
- ☐ Mother's Maiden Name
- ☐ Personal Mailing Address
- ☒ Personal Phone Number(s)
- ☐ Personal Fax Number
- ☐ Personal Email Address
- ☐ Emergency Contact Information (Name, Phone Number, etc. of a different individual)
- ☐ Financial Account Information
- ☐ Health Insurance Beneficiary Numbers 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
- ☐ Gender
- ☐ Integration Control Number (ICN)
- ☐ Military History/Service Connection
- ☐ Next of Kin
- ☒ Other Unique Identifying Information (list below)

OTHER Unique Identifying Info: issue/claim; location (facility, office, department); date of service/issue/close out; resolution facility information; investigation results, actions taken, notes, dates, evidence, and outcomes; risk profile potential prepopulated and structure fields for the use to form a narrative summary/ synopsis, exhibits, or internal documentation & memoranda

**PII Mapping of Components**

CIRTS 2.0 consists of 0 (zero) key components (databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by CIRTS 2.0, and the reasons for the collection of the PII, are in the table below.

**PII Mapped to Components**

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

*PII Mapped to Components*

| Database Name of the information system collecting/storing PII | Does this system collect PII? (Yes/No) | Does this system store PII? (Yes/No) | Type of PII (SSN, DOB, etc.) | Reason for Collection/ Storage of PII | Safeguards |
|---|---|---|---|---|---|
| N/A | N/A | N/A | • N/A | N/A | N/A |

**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.*

Records (or information contained in Records) in this system include allegations made by individuals calling the VHA Office of Compliance and Integrity Help Line, or through another source, to report a possible violation of law, rules, policies, procedures, regulations, or external program requirements such as third-party payer billing guidelines. Records may also contain reports of the reviews or investigations conducted at the medical center, VISN, or Central Office to verify the reported allegations and to take remedial action as needed. Records may also be comprised of inquiries submitted to the Compliance program through the Help Line or through other intake methods as well as intake records pertaining to allegations or inquiries that are ultimately determined to be under the oversight of another program and referred to those programs accordingly.

**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.*

Records (or information contained in Records) in this system include allegations or inquiries made by individuals calling the VHA Office of Integrity and Compliance Help Line, or through another source, including a referral from another program or department, to report, or request information on, a possible violation of law, rules, policies, procedures, regulations, or external program requirements such as third-party payer billing guidelines. Records may also contain reports of the reviews or investigations conducted at the medical center, VISN, or Central Office level to verify the reported allegations, to document the guidance provided to the reporter in the case of an inquiry, or to verify the referral of the allegation or inquiry to the appropriate program or principal office. The records may also contain information pertaining to the resulting causation, corrective and preventive actions stemming from a substantiated allegation.

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

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

*If the system checks for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract.*
*This question is related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.*

On a monthly basis, OIC performs an oversight of CIRTS cases checking the quality of responses and accuracy of data entry with a goal of reviewing at least 35% of all cases annually. Cases fall into two categories: inquiries and allegations. From a qualitative standpoint, (a) inquiries are reviewed to verify that the response is appropriate to the question posed while (b) allegations are reviewed to verify an investigation has been conducted appropriate to the complaint. All data points in all cases are reviewed for accuracy and compared throughout the case for continuity. Oversight reviews are documented and logged via data points within the system and tracked for higher level random review.

**1.5 What specific legal authorities, arrangements, and agreements defined the collection of information?**

*List the full legal authority for operating the system, specifically the authority to collect the information listed in question 1.1. Provide the authorities in a manner understandable to any potential reader, i.e., do not simply provide a legal citation; use statute names or regulations in addition to citations. Legal authorities include Federal laws, regulations, statutes, and Executive Orders.*
*This question is related to privacy control AP-1, Authority to Collect*

The System of Records governing CIRTS 2.0 is 106VA17/74 FR 41490 "Compliance Record, Response, and Resolution of Reports of Persons Allegedly Involved in Compliance Violations—VA". The legal authority to operate the IT system is Title 38 USC Section 501, Title 38 USC 7332, and 45 CFR Parts 160 and 164.

**1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information**

*Consider the specific data elements collected and discuss the potential privacy risks and what steps, if any, are currently being taken to mitigate those identified risks.*

*Consider the following Fair Information Practice Principles (FIPPs) when assessing the risk to individual privacy:*

*Principle of Purpose Specification: Explain how the collection ties with the purpose of the underlying mission of the organization and its enabling authority.*

*Principle of Minimization: Is the information directly relevant and necessary to accomplish the specific purposes of the program?*

*Principle of Individual Participation: Does the program, to the extent possible and practical, collect information directly from the individual?*

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

Follow the format below when entering your risk assessment:
**Privacy Risk:** The CIRTS 2.0 application collects both Personally Identifiable Information (PII) and a variety of other Sensitive Personal Information (SPI). Due to the highly sensitive nature of this data, there is a risk that if the data were accessed by an unauthorized individual or otherwise breached, serious personal, professional or financial harm may result.

**Mitigation:** CIRTS 2.0 employs the standard VA-required security measures for a High-Impact System designed to ensure that the information is not inappropriately disclosed or released. These security measures are specified in the controls VA Directive 6500. VA Handbook 6500

"Risk Management Framework for VA Information Systems – Tier 3: VA Information Security Program".

## 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.*

- **Name:** Used to identify the individual who submits the inquiry to OIC. Also used for other forms of communication.
- **Date of Birth:** Used to identify age and confirm identities of individuals who submit the inquiry to OIC.
- **Personal Phone Number(s):** Used for communication
- **Issue/Claim Number:** Unique identifier for individual inquiries
- **Location (facility, office, department) of Inquiry:** to identify the location of specific facility, office or department involved with inquiry
- **Date of Service or Issue or Closeout:** to identify issue status
- **Resolution Facility Information:** to identify where inquiry issue was resolved
- **Investigation Results, Actions Taken, Notes, Dates, Evidence, and Outcomes:** to keep track of events and status on inquiries
- **Risk Profile Potential:** pre-populated and structural fields for the use to form a narrative data summary or synopsis, exhibits or internal documentation and memoranda

The CIRTS 2.0 application is used by Compliance Officers at each VA Medical Center, VISN and Program Office (as applicable) to record and track the receipt and disposition of reports and/or concerns related to the following VHA areas: enrollment; means testing; eligibility; precertification and certification/utilization review; standards pertaining to documentation, coding and billing; inquiries and remediation; accounts receivable and payable; information protection, record retention, managing requests for information; provider documentation supporting business processes; overpayments; questionable conduct on the part of managers, supervisor or employees as related to business processes; and any other inquiry or allegation relating to the business integrity of VHA operations.

The purpose of the CIRTS 2.0 application is to establish a process to receive reports of suspected compliance violations, and to maintain a system to respond to such allegations. SPI collected is for the purpose of identifying individuals reporting compliance violation, individuals alleged to be involved in compliance violations, and may be recorded in evidentiary records collected while investigating allegations of compliance violations. Also, CIRTS 2.0 will be a central place in

which aggregation of data is kept and maintained in an organized way for meeting proper record retention requirements and eventual transfer and accessioning to National Archives and Records Administration (NARA) in an electronic format per 36 CFR § 1234.6, National Archives and Records Administration.

**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 CIRTS 2.0 application conducts descriptive analysis of the internal data fields to create standardized univariate and bivariate reports at facility, VISN and national levels. These analytic capabilities are native to the CIRTS 2.0 system since it utilizes Cloud Computing. No new information will be created about individuals. PII/SPI information cannot be exported from the CIRTS 2.0 system unless required by law. Aggregated data (at facility, VISN and national levels) can be exported from the CIRTS 2.0 system and linked to external data sources to support root-cause-analysis and quality improvement. The CIRTS 2.0 application utilizes Tableau CRM for the analytics platform, and it is integrated into the application itself. Additional reports can be produced for productivity, effectiveness, risk and trend identification and quality assurance.

**2.3 How is the information in the system secured?**

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

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

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

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

User accounts for the CIRTS 2.0 application are created with specific privileges to user. These accounts are controlled through credentials that are managed by the application. Access to computerized information in the database is restricted to authorized personnel on a need-to-know basis by means of passwords protections, authorized user identification codes and/or PIV card login authentication. Physical access to printouts and data terminals will be limited to authorized personnel in the Compliance Program. Access to physical file folders is restricted to authorized personnel on a need-to-know basis. Paper files are maintained in file cabinets or in closets and are locked at all times and only unlocked for employee access. These files are under the control of the Compliance Officer or his/her designees. VHA buildings are protected from unauthorized access by a protective service and visitors are authorized to enter the building with limited access to VHA office spaces.

Information is collected by Compliance Officers and entered in the CIRTS 2.0 application. Only Compliance Officers will collect PII information and only Compliance Officers have access to enter data into the system.VA, on its own initiative, may disclose records in this system of records in legal proceedings before a court or administrative body after determining that the disclosure of the records to the court or administrative body is a use of the information contained in the records that is compatible with the purpose for which VA collected the records. A data sharing agreement or data use agreement with appropriate data sharing workflow plans may be executed as needed.

**2.4 PRIVACY IMPACT ASSESSMENT: Use of the information. How is access to the PII determined? Are criteria, procedures, controls, and responsibilities regarding access documented? Does access require manager approval? Is access to the PII being monitored, tracked, or recorded? Who is responsible for assuring safeguards for the PII?**

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

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

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

*Principle of Use Limitation: Is the use of information contained in the system relevant to the mission of the project?*
*This question is related to privacy control AR-4, Privacy Monitoring and Auditing, AR-5, Privacy Awareness and Training, and SE-2, Privacy Incident response.*

VA employees can only get licenses to the OARVP platform if they requested the identified POC's within OIC which is just two individuals who are primary and secondary product owners of the system.

## 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*

All electronic data stored in the CIRTS 2.0 system, and paper files, associated with the reported allegation of a VHA compliance violations and generated during the investigative process. Information may be in the form of a narrative summary or synopsis, exhibits, or internal documentation and memoranda. PII and SPI information in the investigation records may include (1) Name; (2) DOB; (3) phone number; (4) issue/claim; (5) location (facility, office, department); (6) date of service/issue/close out; (7) resolution facility information; (8) investigation results, actions taken, notes, dates, evident and outcomes; and (9) risk profile potential.

**3.2 How long is information retained?**

*In some cases, VA may choose to retain files in active status and archive them after a certain period of time. State active file retention periods, as well as archived records, in number of years, for the information and record types. For example, financial data held within your system may have a different retention period than medical records or education records held within your system, please be sure to list each of these retention periods. If the system is using cloud technology, will it be following the NARA approved retention length and schedule?*

*The VA records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented.*
*This question is related to privacy control DM-2, Data Retention and Disposal.*

According to the VHA System of Records Notice (SORN) 106VA17 "Computerized records will be retained indefinitely. Periodic system back-ups will be employed for record protection. If disk space is limited, the records will be archived to tape or disk in accordance with established practice." Paper records will be maintained and disposed of in accordance with VHA Records Control Schedule (RCS 10-1) as authorized and approved by the Archivist of the United States.

**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.*

Salesforce Government Cloud Plus (SFGCP) complies with all VA retention and disposal procedures specified in VA Handbook 6300 and VA Directive 6300. Records contained in the Salesforce FedRAMP cloud will be retained as long as the information is needed in accordance with a NARA-approved retention period. VA manages Federal records in accordance with NARA statues including the Federal Records Act (44 U.S.C. Chapters 21, 29, 31, 33) and NARA regulations (36 CFR Chapter XII Subchapter B). SFGCP records are retained according to Record Control Schedule 10-1 Section 4. (Disposition of Records) (https://www.va.gov/vhapublications/RCS10/rcs10-1.pdf). SFGCP completes a 90-day retention cycle of all data including deletion. Active Data stays on disk until the data is deleted or changed. Customer-deleted data is temporarily available (15 days) from the Recycle Bin. Backups are rotated every 90 days, therefore changed or deleted data older than 90 days is unrecoverable. All data upon completion or termination of a contract will be turned over to VA and disposed of as soon as notice of the termination or completion is given. The 90-day retention schedule refers to how data is retained on the Salesforce FedRAMP cloud. We have no control over this. We will delete records according to the Record Control Schedule 10-1.

**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*

Active Data stays on disk until the VA deletes it. We will not export data for retention. All data will be retained within SFGCP until it is required to be deleted according to the Record Control Schedule 10-1. Data on backups is retained for 90 days until the backups are overwritten. Log data is retained by Salesforce for a year. When hard drives and backup tapes are at their end of life, the media is sanitized based on Salesforce's Media Disposal Policy. Hard drives are overwritten using a multiple---pass write of complementary and random values. If it wipes successfully, we will return the disk or array to the vendor. If it fails during the wiping process we retain and destroy (i.e., degauss, shred, or incinerate). Backup tapes are degaussed prior to disposal. Specifics on the sanitization process are below. Salesforce has an established process to sanitize production backup disks and hard drives prior to disposal, release out of salesforce's control, or release to the vendor for reuse. Production backup disks and hard drives are sanitized or destroyed in accordance with salesforce's Media Handling Process. All data is handled and located in VA own Salesforce's servers in Herndon, VA and Chicago, IL in the Salesforce Government Cloud server classification. Said information is handled with proper authority and scrutiny. Hard drives are sanitized within the data center facility using a software utility to perform a seven---pass overwrite of complementary and random values. If the drives wipe successfully, the hardware will be returned to the lessor. If the drive fails during the wiping process the drives are retained within a locked container within the salesforce data center

facilities until onsite media destruction takes place. Leasing equipment provides salesforce with the opportunity to use the latest equipment available from vendors. Periodically, a third-party destruction vendor is brought on---site to perform physical destruction of any hard drives that failed overwrite. A certificate of destruction is issued once the media is physically destroyed. Electronic data and files of any type, including PII, Sensitive Personal Information (SPI), and more are destroyed in accordance with the Department of Veterans' Affairs Handbook 6500.1, Electronic Media Sanitization.

When required, this data is deleted from their file location and then permanently deleted from the deleted items and recycling bin. Magnetic media is wiped and sent out for destruction per VA Handbook 6500.1. Digital media is shredded or sent out for destruction per VA Handbook 6500.1. The OIT Chief/CIO will be responsible for identifying and training OIT staff on VA media sanitization policy and procedures. The ISO will coordinate and audit this process and document the audit on an annual basis to ensure compliance with national media sanitization policy. Paper records at the end of their retention period that are eligible for destruction are destroyed by shredding. The shredding company is determined by the shredding contract at facility where each respective OIC office is located, and all documentation regarding shredding is controlled by that facility as one entity.

**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*

Information is not repurposed for research and testing. As no training environment exists, new staff will be trained in the live system. However, their permission set would limit them to view-only data to which they have appropriate access. All staff trainings carefully select records used as examples.

**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 risk to maintaining data within the Master Person Index (MPI) is that longer retention times increase the risk that information can be compromised or breached. Risks of retaining data in an e-system usually includes: (1) the risk of inappropriate access, (2) the risk of record tempering, and (3) the risk of record loss due to natural catastrophes.

**Mitigation:** OIC collects only the data necessary for investigations. Information is collected by Compliance Officers and/or Compliance Staff and entered into the CIRTS 2.0 application. Only Compliance personnel have access to the system as granted through approved licensing. All electronic storage media used to store, process, or access OIC records will be stored in adherence with the latest version of VA Handbook 1605.01, Privacy and Release of Information.

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

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

**4.1 With which internal organizations is information shared/received/transmitted? What information is shared/received/transmitted, and for what purpose? How is the information transmitted?**

**NOTE: Question 3.9 (second table) on Privacy Threshold Analysis should be used to answer this question.**

*Identify and list the names of any program offices, contractor-supported IT systems, and any other organization or IT system within VA with which information is shared.*

*State the purpose for the internal sharing. If you have specific authority to share the information, provide a citation to the authority.*

*For each interface with a system outside your program office, state what specific data elements (PII/PHI) are shared with the specific program office, contractor-supported IT system, and any other organization or IT system within VA.*

*Describe how the information is transmitted. For example, is the information transmitted electronically, by paper, or by some other means? Is the information shared in bulk, on a case-by-case basis, or does the sharing partner have direct access to the information?*
*This question is related to privacy controls AP-2, Purpose Specification, AR-3, Privacy Requirements for Contractors and Service Providers, AR-8, Accounting of Disclosures, TR-1, Privacy Notice, and UL-1, Internal Use.*

*Data Shared with Internal Organizations*

| ***List the Program Office or IT System information is shared/received with*** | ***List the purpose of the information being shared /received with the specified program office or IT system*** | ***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system*** | ***Describe the method of transmittal*** |
|---|---|---|---|
| Identity and Access Management (IAM) - Active Directory Federated Service (ADFS) | IAM ADFS Provisioning Service provides self-service options for internal VA users for centralized creation, modification, deletion, and suspension for user accounts based on business processes and interactions defined by applications or systems. | ADFS sends the SAML assertion to the Salesforce based on the user credentials validated at the Identity Provider. The SAML Assertion contains the Federation ID in the User object.<br><br>• Federation ID<br>• Name<br>• DOB<br>• Phone Number | Access credentials via login credentials along with integrating the PIV card and eToken security fobs. |
| Master Person Index (MPI) | Verify Veteran Status | • Name<br>• DOB<br>• Phone Number<br>• Mailing Address | Bidirectional system interface via MPI |

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

*Discuss the privacy risks associated with the sharing of information within the Department and what steps, if any, are currently being taken to mitigate those identified risks.*
*This question is related to privacy control UL-1, Internal Use.*

Follow the format below:
**Privacy Risk:** There is a risk that information may be shared with unauthorized VA program or system or that data could be shared.

**Mitigation:** Safeguards implemented to ensure data is not sent to the wrong VA organization are employee security and privacy training and awareness and required reporting of suspicious activity. Use of secure passwords, access for need-to-know basis, PIV Cards, PIN numbers, encryption, and access authorization are all measures that are utilized within the facilities.

## Section 5. External Sharing/Receiving and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to VA, which includes Federal, State, and local governments, and the private sector.

**5.1 With which external organizations (outside VA) is information shared/received? What information is shared/received, and for what purpose? How is the information transmitted and what measures are taken to ensure it is secure?**

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

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

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

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

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

*Describe how the information is transmitted to entities external to VA and what security measures have been taken to protect it during transmission.*
*This question is related to privacy control UL-2, Information Sharing with Third Parties*

*Data Shared with External Organizations*

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

**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

**Mitigation:** N/A

## Section 6. Notice

The following questions are directed at providing notice to the individual of the scope of information collected, the right to consent to uses of the information, and the right to decline to provide information.

**6.1 Was notice provided to the individual before collection of the information? If yes, please provide a copy of the notice as an appendix. (A notice may include a posted privacy policy, a**

**Privacy Act notice on forms, or a system of records notice published in the Federal Register.) If notice was not provided, why not?**

*This question is directed at the notice provided before collection of the information. This refers to whether the person is aware that his or her information is going to be collected. A notice may include a posted privacy policy, a Privacy Act statement on forms, or a SORN published in the Federal Register. If notice was provided in the Federal Register, provide the citation.*

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

*Describe how the notice provided for the collection of information is adequate to inform those affected by the system that their information has been collected and is being used appropriately. Provide information on any notice provided on forms or on Web sites associated with the collection. This question is related to privacy control TR-1, Privacy Notice, and TR-2, System of Records Notices and Privacy Act Statements, and TR-3, Dissemination of Privacy Program Information.*

Yes. For OIC Helpline purposes, individuals are informed and aware their reports are being tracked in CIRTS 2.0 for an investigation and response, and they are provided with a CIRTS 2.0 reference number which indicates which report houses the data they provide. OIC's and Compliance Professionals in the field conducting investigations notify appropriate individuals of the information necessary to proceed with the investigation. VA also provides notice to Veterans and their dependents on what information is collected on them and what that information is used for. This notice is provided in the Notice of Privacy Practices VA 10-163. Link provided in the appendix.

**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*

Yes, reporters of allegations may remain anonymous throughout the reporting process. Reporters are notified that by remaining anonymous or declining to provide information that an investigation may not be able to be processed completely. During an investigation, an individual may decline to provide information. A penalty or denial of service is not attached; however, the denial of information is documented in CIRTS 2.0 to provide a paper trail of workflow. In this event, if fraudulent activity is suspected and OIC's investigation is halted, OIC notifies VA OIG of the reported allegation for action as needed.

**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*

There are no particular uses of CIRTS 2.0 data that necessitate consent from Veterans. As information in the CIRTS 2.0 system is entered into the system due to compliance allegations or claims that require investigation. In addition, information will not be shared with, or accessible by, any other entity without prior approval from OIC and review of data security and safety plans. All known efforts will be used to mitigate compromising the use of PHI/PII/SPI.

### 6.4 PRIVACY IMPACT ASSESSMENT: Notice

*Describe the potential risks associated with potentially insufficient notice and what steps, if any, are currently being taken to mitigate those identified risks.*

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

*Principle of Transparency: Has sufficient notice been provided to the individual?*

*Principle of Use Limitation: Is the information used only for the purpose for which notice was provided either directly to the individual or through a public notice? What procedures are in place to ensure that information is used only for the purpose articulated in the notice?*
*This question is related to privacy control TR-1, Privacy Notice, AR-2, Privacy Impact and Risk Assessment, and UL-1, Internal Use*

Follow the format below:
**Privacy Risk:** There is a risk that veterans and other members of the public will not know that the CIRTS 2.0 exists or that it collects, maintains, and/or disseminates Personally Identifiable Information (PII) and other Sensitive Personal Information (SPI) about them.

**Mitigation:** Individuals are informed and aware that identifying information they provide is tracked in CIRTS 2.0 for an investigation and response, and they are provided with a CIRTS 2.0 issue/claim number which indicates which report houses the data they provide. There are no particular uses of CIRTS 2.0 data to necessitate consent. PHI/PII is not being compromised.

This PIA is published where it accessible to the public and serves as a notice with details about this system and the information contained within it. A System of Records Notice (SORN), 106VA17 which applies to the information in this system, has also been published in the Federal Register and is available to the public at https://www.govinfo.gov/content/pkg/FR-2009-08-17/pdf/E9-19628.pdf.

## 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.*

Requestors may submit a Freedom of Information Act (FOIA) request as follows. Submitting a written FOIA request signed by the requestors and reasonably describing the records sought to the VHA Central Office FOIA Service at 810 Vermont Avenue, NW (10A7) Washington, DC 20420, by fax at 202-273-9381, or via email at vhafoia2@va.gov. The VHA FOIA Office will obtain the requested records from the VHA Office of Integrity and Compliance (OIC) and respond to the request as permitted under the FOIA.

Under the Privacy Act, the subject of the record (First Party Access) or appropriate designee (Third Party Access) may request their own identifiable information from CIRTS 2.0. In addition, Information collected in CIRTS 2.0 may be shared with VHA employees, contractors, and other service providers as necessary to respond to a request, provide a service, administer clinical treatment, solicit payment or as otherwise authorized by law for their official duties. Information will not be shared with, or accessible by, any other entity without legal authority and prior approval from OIC and review of data security and safety plans.

**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.*

An individual who seeks access to or wishes to contest records maintained under his or her name in this system may write, call, or visit the VHA Office of Integrity and Compliance (10OIC) Department of Veterans Affairs, 810 Vermont Avenue, NW. Washington, DC 20420. 202-745-8000 Ext. 55533.

### 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.*

Individuals are provided with a CIRTS 2.0 issue/claim number which indicates which report houses the data they provide. An individual who seeks access to or wishes to contest records maintained under his or her name in this system may write, call, or visit the VHA Office of Integrity and Compliance (10OIC) Department of Veterans Affairs, 810 Vermont Avenue, NW. Washington, DC 20420. 202-745-8000 Ext. 55533.

Veterans are informed of the amendment process by many resources to include the VA Notice of Privacy Practice (NOPP), IB 10-163, which states:

**Right to Request Amendment of Health Information**
You have the right to request an amendment (correction) to your health information in our records if you believe it is incomplete, inaccurate, untimely, or unrelated to your care. You must submit your request in writing, specify the information that you want corrected, and provide a reason to support your request for amendment. All amendment requests should be submitted to the facility Privacy Officer at the VHA health care facility that maintains your information.
If your request for amendment is denied, you will be notified of this decision in writing and provided appeal rights. In response, you may do any of the following:
• File an appeal
• File a "Statement of Disagreement"
• Ask that your initial request for amendment accompany all future disclosures of the disputed health information. Information can also be obtained by contacting the facility ROI office.

### 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.*

Veterans and other individuals are encouraged to use the formal redress procedures discussed above to request edits to their personal medical records and other personal records retained about them.

An individual who seeks access to or wishes to contest records maintained under his or her name in this system may write, call, or visit the VHA Office of Integrity and Compliance (10OIC) Department of Veterans Affairs, 810 Vermont Avenue, NW., Washington, DC 20420. 202-745-8000 Ext. 55533.

**7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction**

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

*Consider the following FIPPs below to assist in providing a response:*
*Principle of Individual Participation: Is the individual provided with the ability to find out whether a project maintains a record relating to him?*

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

*Principle of Individual Participation: Is there a mechanism by which an individual is able to prevent information about him obtained for one purpose from being used for other purposes without his knowledge?*
*This question is related to privacy control IP-3, Redress.*

Follow the format below:
**Privacy Risk:** There is a risk that individuals whose records contain incorrect information may not receive notification on their issue/claim.

**Mitigation:** Individuals are informed and aware that identifying information they provide is tracked in CIRTS 2.0 for investigation and response purposes. An individual may file a Privacy Act request and Freedom of Information Act (FOIA) request for information about them. Privacy Act and Freedom of Information Act requirements are followed in providing this information to an individual. CIRTS 2.0 data is not routinely shared with other entities, and there is no access to the CIRTS 2.0 system outside of OIC Compliance Officers and OI&T System Administrators.

## 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.*

Only OIC Compliance Officers and approved Compliance personnel have access the CIRTS 2.0 system. No other individuals or persons have access to the CIRTS 2.0 system or information, except for OI&T System Administrators for the purposes of computer system administration, management, and maintenance. User accounts are created with specific privileges to the application. In an event the user is inactive in their account for 90 days or more, the user's access will be revoked. Once the access is revoked, the user will have to request reactivation of their access from the system administrator. These accounts are controlled through credentials that are managed by the application. Access to computerized information in the database is restricted to authorized personnel on a need-to-know basis. User accounts are provisioned and governed by VA IT via Single-Sign-On (SSO) to the SFGCP platform. Physical access to printouts and data terminals is limited to authorized personnel in the Compliance Program. Access to paper file folders is restricted to authorized personnel on a need-to-know basis. Paper files are maintained in file cabinets or closets and are locked after duty hours. These files are under the control of the Compliance Officer or his/her designees at the respective OIC locations.

**8.2 Will VA contractors have access to the system and the PII? If yes, what involvement will contractors have with the design and maintenance of the system? Has a contractor confidentiality agreement, Business Associate Agreement (BAA), or a Non-Disclosure Agreement (NDA) been developed for contractors who work on the system?**

*If so, how frequently are contracts reviewed and by whom? Describe the necessity of the access provided to contractors to the system and whether clearance is required. If Privacy Roles and Responsibilities have been established to restrict certain users to different access levels, please describe the roles and associated access levels. Explain the need for VA contractors to have access to the PII.*

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

The Compliance Inquiry Reporting & Tracking System (CIRTS 2.0) will be built on Salesforce.com, a cloud-based Software as a Service (SaaS) platform. Contractors will have access to the system, PII, PSI and EPHI as the platform is built. Contractors in collaboration with VA Personnel are responsible for designing the system and providing on-going maintenance. Privacy & HIPAA Training outlines VA Privacy and Information Security Awareness and Rules of Behavior, as well as the Health Insurance Portability and Accountability Act (HIPAA) training requirements. The contractors who provide support to the system are required to complete annual VA Privacy and information Security and Rules of Behavior training via the VA's Talent Management System (TMS). The Office of Contract Review operates under a reimbursable agreement with VA's Office of Acquisition, Logistics and Construction (OALC) to provide pre-award, post-award, and other requested reviews of vendors' proposals and contracts.

All contractors must comply with Appendix C of VA Handbook 6500.6, Contract Security. Additionally, in section A5.0, pages 52-54, Confidentiality and Non-Disclosure, outlines contractor requirements with regards to complying with VA rules and regulations regarding information security to prevent disclosure of sensitive information to unauthorized individuals or organizations.

Contractor performance is reviewed annually by the Contract Officer Representative (COR), Contract Specialist (CS) and Contract Officer (CO). The System Owner and Contracting Officer Representative (COR) is the individual to accept and amend any incoming or outgoing contracts involving Salesforce Development Platform VA.

**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.*

The TMS course "VA Privacy and Information Security Awareness and Rules of Behavior" is an annual VA requirement. Health Insurance Portability and Accountability Act (HIPAA) training is also required.

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

*If Yes, provide:*

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

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

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

**CIRTS 2.0 went into production on 11/12/2021.**

1. The Security Plan Status: Approved
2. The Security Plan Status Date: 02/24/2021
3. The Authorization Status: ATO
4. The Authorization Date: 03/18/2021
5. The Authorization Termination Date: 12/17/2023

6. The Risk Review Completion Date: 03/12/2021
7. The FIPS 199 classification of the system: MODERATE (M/M/M – C/I/A)

## Section 9 – Technology Usage

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

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

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

*This question is related to privacy control UL-1, Information Sharing with Third Parties.*

*Note: For systems utilizing the VA Enterprise Cloud (VAEC), no further responses are required after 9.1.*

Yes, CIRTS 2.0 utilizes Salesforce Government Cloud Plus (SFGCP). SFGCP is hosted in the AWS GovCloud. The Salesforce Government Cloud Plus (SFGCP-E) is built on the underlying Salesforce Force.com that is hosted in a FedRAMP Certified FISMA High environment which is in the Amazon Web Services (AWS) GovCloud West. This software utilizes the PaaS Service of Salesforce Government Cloud Plus Platform.

**9.2 Does the contract with the Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII? (Provide contract number and supporting information about PII/PHI from the contract)**

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

Yes, VA has full ownership of the PII that will be shared through the CIRTS 2.0 platform. Contract agreement “Salesforce Subscription Licenses, Maintenance and Support”, Contract Number: NNG15SD27B.

**9.3 Will the CSP collect any ancillary data and if so, who has ownership over the ancillary data?**

*Per NIST 800-144, cloud providers hold significant details about the accounts of cloud consumers that could be compromised and used in subsequent attacks. Ancillary data also involves information the cloud provider collects or produces about customer-related activity in the cloud. It includes data collected to meter and charge for consumption of resources, logs and*

*audit trails, and other such metadata that is generated and accumulated within the cloud environment.*

*This question is related to privacy control DI-1, Data Quality.*

No, this system does not collect ancillary data.

**9.4 NIST 800-144 states, "Organizations are ultimately accountable for the security and privacy of data held by a cloud provider on their behalf." Is this principle described in contracts with customers? Why or why not?**

*What are the roles and responsibilities involved between the organization and cloud provider, particularly with respect to managing risks and ensuring organizational requirements are met?*

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

Yes, OARVP CIRTS 2.0 utilizes Salesforce Government Cloud Plus platform. VA has full authority over data stored in CIRTS 2.0.

**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).*

No, CIRTS 2.0 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 provided in this Privacy Impact Assessment is true and accurate.**

Phillip Cauthers 255139

Digitally signed by Phillip Cauthers 255139
Date: 2022.08.02 08:42:18 -07'00'

**Privacy Officer, Phillip Cauthers**

JAMES BORING

Digitally signed by JAMES BORING
Date: 2022.08.02 12:23:14 -04'00'

**Information Systems Security Officer, James Boring**

Michael S. Domanski 326889

Digitally signed by Michael S. Domanski 326889
Date: 2022.08.08 10:33:03 -04'00'

**Information System Owner, Michael Domanski**

## APPENDIX A-6.1

Please provide a link to the notice or verbiage referred to in Section 6 (a notice may include a posted privacy policy, a Privacy Act notice on forms).

System of Record Notice 106VA17 / FR41490 ‘‘Compliance Records, Response, and

Notice_of_Privacy_Practices_VA_-_IB_10-163.pdf

VA Handbook 6500 Electronic Media Sanitation