Privacy Impact Assessment for the VA IT System called:

Salesforce - VA Integrated Enterprise Workflow Solution Case and Correspondence Management

Office of the Executive Secretariat (EXECSEC)

VA Central Office (VACO)

Date PIA submitted for review:

9/15/2022

System Contacts:

<table>
<thead>
<tr>
<th>System Contact</th>
<th>Name</th>
<th>E-mail</th>
<th>Phone Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy Officer</td>
<td>Gina Siefert</td>
<td><a href="mailto:Gina.Siefert@va.gov">Gina.Siefert@va.gov</a></td>
<td>202-632-8430</td>
</tr>
<tr>
<td>Information System Security Officer (ISSO)</td>
<td>James Boring</td>
<td><a href="mailto:James.Boring@va.gov">James.Boring@va.gov</a></td>
<td>215-842-2000 x4613</td>
</tr>
<tr>
<td>Information System Owner</td>
<td>Michael Domanski</td>
<td><a href="mailto:Michael.Domanski@va.gov">Michael.Domanski@va.gov</a></td>
<td>727-595-7291</td>
</tr>
</tbody>
</table>
Abstract

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

Salesforce - VA Integrated Enterprise Workflow Solution Case and Correspondence Management (VIEWS CCM) is used by the Office of the Executive Secretariat (EXECSEC) and VA staff and program offices to conduct administrative and correspondence-related work. VIEWS CCM is also used to coordinate documents and materials related to partnerships with other Federal organizations, state, local, tribal, and non-governmental organizations (NGOs) and individuals, as well as international governments and private sector organizations. VIEWS CCM is used to manage Congressional correspondence; internal documents such as reports, memoranda, and handbooks; respond to White House case mail; and assist Veterans making inquiries about our programs, services, and benefits. VIEWS CCM is used by all VA administrations, program, and staff offices and is a NARA-certified system of record.

Overview

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

- The IT system name and the name of the program office that owns the IT system.
- The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission.
- Indicate the ownership or control of the IT system or project.
- The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.
- A general description of the information in the IT system and the purpose for collecting this information.
- Any information sharing conducted by the IT system. A general description of the modules and subsystems, where relevant, and their functions.
- Whether the system is operated in more than one site, and if so, a description of how use of the system and PII is maintained consistently in all sites and if the same controls are used across sites.
- A citation of the legal authority to operate the IT system.
- Whether the completion of this PIA will result in circumstances that require changes to business processes.
- Whether the completion of this PIA could potentially result in technology changes.
- If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval? If the system is using cloud technology, does the SORN for the system cover cloud usage or storage?
VIEWS CCM supports Case and Correspondence Management within the VA and with the Veteran. The system facilitates correspondence of any form (emails, letters and any other communication internal or external to the VA), workflow/tasking, case management and project/event tracking. VIEWS CCM also provides managers with robust reporting, data management and business intelligence capabilities to drive informed decision-making. The Office of the Executive Secretariat (EXECSEC) is the VIEWS CCM business owner. The Office of Information and Technology (OIT) is the system owner.

The VIEWS CCM Case Management process includes the following steps in the end-to-end case life cycle: case creation upon receipt of congressional correspondence/email; case intake assessment with addition of related details, liaison and Subject Matter Expert (SME) tasking; case communications tracking, liaison response and concurrence; Office of General Council (OGC) response approval; 0907 process enabling Congressional Letter Response circulation for physical signature; and case closure.

VIEWS CCM stores information on system users and other persons who have initiated a case or are involved in subsequent processing. There are approximately 1,800 system users. Currently, 300,000 to 400,000 persons’ information may be stored in the system. These individuals, which could include any Veteran or other persons (VA employees and contractors) that have business with the Department, are related to the correspondence received by the VA.

VIEWS CCM collects, processes or retains information on Veterans and/or dependents, as well as VA employees and contractors. Data entered into this system is directly related to the correspondence received, including information on the person who sent the request and information in the correspondence. As the correspondence is being tracked, additional information may be added to the system in regard to the response of the question(s).

Case records contain information about the case’s description, including contacts, Veteran (if applicable), case progress, associated VA facilities, related emails and attachments (associated documents), and other details.

Each case is assigned a type, which can refer to external (Veteran, Congressional or Presidential) or internal documents (such as memos, reports, handbooks or correspondence). A case team consists of organizations (queues) or individuals that will work on a case. They can be added or removed as necessary by the case owner, other case team members and office coordinators. Case tasks are actions that are taken and assigned to case team members or other users, such as reviewing, concurring, signing or closing.

VIEWS CCM objects contain VA staff and system user identifiers, case emails, case queue ownership, case notes, case teams, associated contacts, contact roles and functional queue members. VIEWS CCM users can view all cases. Restrictions to related records are applied when the case sensitivity is marked as ‘Pending Review’ or ‘Sensitive.’ Case Notes are used to capture sensitive information that should not be on the case. Users can send email only to permitted VA accounts.

The system shares information with Identity and Access Management (IAM) and the Master Person Index (MPI), also called Master Veterans Index (MVI) to validate the Veteran’s identity. MPI is the
VA’s authoritative source for personal identity data, providing a universal, unique identification record for Veterans. The MPI integration in VIEWS CCM also serves as a searchable database of verified Veteran contact information. VIEWS CCM uses the MPI to verify a Veteran’s identity, attach the Veteran to the case and view existing cases associated with the Veteran. MPI information includes name, email, last four digits of social security number (SSN), birth date and eligibility status. The legal authority is 38 U.S.C. 7601-7604 and U.S.C 7681-7683 and Executive Order 9397.

The MVI Integration Control Number (ICN) is the external ID stored on the Contact object in Salesforce. This is the person record identifier between MPI and Salesforce. Additional Sensitive Personal Information (SPI) may include Military Service History, Branch of Service, Place of Birth, Education History, Employment History and Gender.

All VA administrations and program and staff offices use VIEWS CCM. System users may also log in remotely. VIEWS CCM is operated at VA Central Office (VACO) in several Washington, DC locations. User controls built into the system manage Personally Identifiable Information (PII) identically at all locations. No regions, hospitals, medical centers or any other agency use the system.

KnowWho is a Salesforce App Exchange product that provides a directory of contact and biographical data on all Members of Congress (MOC), Capitol Hill staffers, committees and caucuses. The KnowWho integration allows case owners to search for and attach MOC, their staffers and other VA facilities directly to a case as an Associated Contact. The KnowWho database includes physical and mailing addresses, phone and fax numbers, email addresses, social media URLs, committee memberships and other information. Congressional data provided by KnowWho is used to coordinate legislative proposals, manage activities with Congress or respond to congressional constituents. The directory delivers daily updates to VIEWS CCM as a commercial service. KnowWho uses Salesforce standard objects for loading publicly available PII.

The Functional Operation Manual (FOM), another VIEWS CCM integration, maintains a hierarchy of organizations (queues) that can be assigned to a case. A VIEWS CCM user can associate persons within an organization to a case via Case Team functionality.

VIEWS CCM runs in the Salesforce Government Cloud Plus (SFGCP). Salesforce has been FedRAMP-certified for Platform as a Service (PaaS) and Software as a Service (SaaS) since 2014. All Salesforce Government Cloud Plus customers are on the same version, patch set and code base, minimizing security risk and lowering complexity. More than 40 other Federal agencies have issued an Authority To Operate (ATO) for solutions deployed on the Salesforce Government Cloud Plus. In addition, security levels and permissions have been implemented to ensure workflow owners have access to the information they need while protecting sensitive data, such as PII and Protected Health Information (PHI). VIEWS CCM (VASI ID 2619) was developed and built using the Salesforce Government Cloud Plus Platform, which is Federal Risk and Authorization Management Program (FedRAMP) Moderate approved. It is hosted on the U.S. Government Cloud Plus (FedRAMP High), built on Amazon Web Services (AWS) GovCloud (U.S.). It is classified as a Minor application that augments the Major Application SFDP.
VIEWS CCM has a FedRAMP agency authorization date of November 2, 2020. The Federal Information Processing Standards (FIPS) 199 classification is Moderate. An ATO was granted on March 18, 2021 and expires on December 17, 2023.

Salesforce’s Master Subscription Agreement addresses the protection of Customer Data. A sample Master Subscription Agreement can be viewed here:

http://www.salesforce.com/assets/pdf/misc/salesforce_MSA.pdf

In addition to the Master Subscription Agreement, Salesforce has documented a System Security Plan that identifies the documented security controls protect the environment in which Customer Data is stored. Additionally, their privacy and security statements can be viewed here:

http://www.salesforce.com/company/privacy

Salesforce has a global privacy team that oversees privacy for Salesforce. Protecting the security and privacy of user data is a shared responsibility between Salesforce and the VA.

Salesforce Government Cloud Assessing was granted a full ATO by Deputy Chief Information Officer (CIO) Service Delivery and Engineering (SD&E). The Salesforce Government Cloud Assessing maintains an underlying physical infrastructure. Additional Industry Standard Architecture/Memoranda of Understanding (ISA/MOUs) are required between the VA and VA-designated contractors/vendors who own the data that is stored or processed within Salesforce Development Platform VA Assessing. The vendor-specific agreements describe the data ownership and storage requirements. The parties agree that transmission, storage and management of VA sensitive information residing in the Salesforce Development Platform VA Assessing is the sole responsibility of VA employees or designated contractors/vendors assigned to manage the system.

At no time will Salesforce Government Cloud Assessing have any access to VA data residing within the Salesforce Development Platform VA Assessing. Thus, all agreements on data and system responsibilities shall not be covered in the base agreement (MOU). However, Salesforce Government Cloud Assessing provides the tools to allow VA to properly secure all systems and data hosted in the Salesforce Development Platform VA Assessing.

The following is a full list of related laws, regulations and policies and the legal authorities:

- Title 38, United States Code, Sections 501(a), 1705, 1710, 1722, and 5317
- Information Technology Management Reform Act of 1996 (also known as the Clinger-Cohen Act)
- Federal Information Security Management Act (FISMA) of 2002
The following System of Records related to VIEWS CCM:
75VA001B/87 FR 36584

The VA Salesforce contract establishes VA ownership rights of all data. The contract stipulates that the contractor shall not retain any copies of data, in full or in part, at the completion of the performance period. The data shall contain no proprietary elements that would preclude the VA from migrating the data to a different hosting environment or from using a different case management system in the future.

The Salesforce contract addresses the National Institute of Standards (NIST) 800-144 principle that states, “Organizations are ultimately accountable for the security and privacy of data held by a cloud provider on their behalf.”

If privacy-related data is disclosed, intentionally or unintentionally, VA would incur significant harm to its reputation, and violators may be held responsible with potential civil or criminal liabilities. In addition, VA could be compelled to provide credit monitoring services and other compensation to any customers who were thus harmed. Depending on the circumstances and root cause of a privacy disclosure incident, the cloud service provider’s reputation could be damaged.

Completion of this PIA is not expected to require changes to any technology or business processes.
System of Record Notice (SORN):
75VA001B/87 FR 36584

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://www.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)

PII Mapping of Components

VIEWS CCM consists of one key component: Salesforce Government Cloud Plus. This component has been analyzed to determine if any elements collect PII. The type of PII collected by VIEWS CCM and the reasons for the collection of the PII are described in the following table.

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

<table>
<thead>
<tr>
<th>Database Name of the information system collecting/storing PII</th>
<th>Does this system collect PII? (Yes/No)</th>
<th>Does this system store PII? (Yes/No)</th>
<th>Type of PII (SSN, DOB, etc.)</th>
<th>Reason for Collection/Storage of PII</th>
<th>Safeguards</th>
</tr>
</thead>
<tbody>
<tr>
<td>VA Salesforce Development Platform (SFDP) VA SFGCP, via Business Partner Extranet (BPE) Connection</td>
<td>Yes</td>
<td>Yes</td>
<td>Name, Gender, Personal Phone, Personal Email, Date of Birth, Personal Mailing Address, Emails, Military Service History, Branch of Service, Place of Birth, Education History, Master Person Index and Employment History</td>
<td>To support case and correspondence management within the VA and with the Veteran</td>
<td>Access to VIEW S CCM is strictly controlled by Single Sign On (SSO) to authorized VA personnel only. Salesforce is FedRAMP (Moderate) approved. SFGCP uses cryptography that is compliant with Federal laws and regulations FIPS 140-2. All PII is encrypted in transport and at rest. Profile-based permissions govern access. User profiles are reviewed regularly to ensure appropriate access. VA employees and contractors are required to complete the VA Privacy and Information Security training annually.</td>
</tr>
</tbody>
</table>
1.2 What are the sources of the information in the system?

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

Describe why information from sources other than the individual is required. For example, if a program’s system is using data from a commercial aggregator of information or data taken from public Web sites, state the fact that this is where the information is coming from and then in question 1.3 indicate why the system is using this source of data.

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

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

The system receives information from the entry of cases with data provided from any type of correspondence with the VA (email, regular mail, phone call, and so on). Additionally, the system consumes Global Address List (GAL) (Outlook email account) data that contains email and work phone number information for VA employees and contractors. Veteran information is brought into the system via lookup through a real-time interface with MPI.

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.

Information in the VIEWS CCM application is manually entered or uploaded as documents by an authorized VIEWS CCM user, who is a VA employee or contractor. Email-to-case functionality allows related emails to be entered with the case. In the cases where validation of Veteran status is needed, the information and data will be collected from the incoming correspondence and validated by the system’s access to the MI integration. Information that cannot be validated will be saved as non-verified, and contact information will be retained for the correspondence.

If Congressional data is needed for a case, KnowWho provides a lookup capability of biographical data on all MOCs, Capitol Hill staffers, committees and caucuses.
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.

VIEWS CCM uses the MPI database to verify and confirm Veteran identity. The VIEWS CCM user interface includes a visual workflow for users to enter social security number and date of birth, which makes a call to the MPI database to verify the identity and pull the information into a verified Veteran contact record type. The contact record is marked as a verified Veteran and contains the MPI external ID, which is used to match against the MPI database and update information from MPI to Salesforce.

Other SPI information may be stored as part of routine case management but not validated by the system for data accuracy or corruption.

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

- No. 104-231, 110 Stat. 3048
- 5 U.S.C. § 552a, Privacy Act of 1974, As Amended
- Public Law 100-503, Computer Matching and Privacy Act of 1988
- E-Government Act of 2002 § 208
- Federal Trade Commission Act § 5
- 44 U.S.C. Federal Records Act, Chapters 21, 29, 31, 33
- Title 35, Code of Federal Regulations, Chapter XII, Subchapter B
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:** SPI, including personal contact information, SSN and medical information, may be released to unauthorized individuals.

**Mitigation:** Profile-based permissions govern user access to information. The profiles are reviewed on a regular basis to ensure that information is shared only with appropriate users. All employees with access to Veterans’ information are required to complete the VA Privacy and Information Security Awareness and Rules of Behavior training annually.

**Privacy Risk:** Unsecured SPI, including personal contact information, SSN and medical information, may be exposed.

**Mitigation:** VIEWS CCM ensures that only authorized users can access SPI. Assigned data security rules determine which data users can access. All data is encrypted in transfer. Access is
governed by strict password security policies. All passwords are stored in Secure Hash Algorithm (SHA) 256 one-way hash format.

**Privacy Risk:** Facility-wide data breach.

**Mitigation:** To ensure the utmost privacy and security facility-wide, authorized personnel must pass through multiple levels of biometric and/or badge scanning to reach the Salesforce system rooms/cages. All buildings are completely anonymous, with bullet-resistant exterior walls and embassy-grade concrete posts and planters around the perimeter. All exterior entrances feature silent alarm systems that notify law enforcement in the event of a suspected intrusion. Data is backed up. Backups do not physically leave the data center.

**Privacy Risk:** Data breach at the network level.

**Mitigation:** Multi-level security products from leading vendors and proven security practices ensure network security. To prevent malicious attacks through unmonitored ports, external firewalls allow only Hypertext Transfer Protocol Secure (https) traffic on the correct ports, along with Internet Control Message Protocol (ICMP) traffic. Switches ensure that the network complies with the Request for Comment (RFC) 1918 standard and address translation technologies further enhance network security. Intrusion Detection Sensors protect all network segments. Internal software systems are protected by two-factor (2FA) authentication, along with the extensive use of technology that controls points of entry.

**Section 2. Uses of the Information**

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

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

*Identify and list each use (both internal and external to VA) of the information collected or maintained.*

*This question is related to privacy control AP-2, Purpose Specification.*

User-level data is necessary for provisioning VIEWS CCM and providing the service. User-level data may include:

- **Name:** Identifies the Veteran and retained for provider reference and reporting.
- **Last four digits of Social Security Number:** Unique Veteran identifier and retained for provider visit record.
- **Date of Birth:** Identifies Veteran’s age and retained for provider reporting and awareness.
- **Mother’s Maiden Name:** Identifies the Veteran and retained for provider reference.
• **Mailing Address**: Used for communication and retained for provider reporting.
• **Phone Number(s)**: Used for communication and retained for provider reporting.
• **Fax Number**: Used for communication and retained for provider reporting.
• **Email Address**: Used for communication and retained for provider reporting.
• **Emergency Contact Information**: (Name, Phone Number, etc. of a different individual).
• **Financial Account Information**: May be included if relevant to the case created.
• **Health Insurance Beneficiary Numbers**: May be included if relevant to the case created.
• **Certificate/License Numbers**: May be included if relevant to the case created.
• **Vehicle License Plate Number**: May be included if relevant to the case created.
• **Internet Protocol Address**: Identifies the Veteran’s network interface and location addressing.
• **Current Medications**: May be included if relevant to the case created.
• **Previous Medical Records**: May be included if relevant to the case created.
• **Race/Ethnicity**: Identifies the Veteran and retained for provider reference.
• **Tax Identification Number**: May be included if relevant to the case created.
• **ICN**: Lookup number for MPI used internally within the system for data consistency.
• **Military Service History**: May be included if relevant to the case created.
• **Branch of Service**: May be included if relevant to the case created.
• **Place of Birth**: Identifies the Veteran’s birthplace.
• **Education History**: May be included if relevant to the case created.
• **Employment History**: May be included if relevant to the case created.
• **Gender**: Identifies the Veteran and retained for provider reference.

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.
VIEWS CCM does not include tools to perform complex analytical tasks resulting in, among other types of data, matching, relational analysis, scoring, reporting or pattern analysis.

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

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.

VIEWS CCM utilizes the Salesforce Government Cloud Plus. Users must be approved by their manager in order to have a user login created. Once access is granted, users must log into Salesforce via Single Sign On (SSO) for verification.

Controls are in place to ensure data is used and protected in accordance with legal requirements, VA policies and VA’s stated purpose for data usage. Controls include mandatory training completion for all employees, volunteers and contractors.
All system access is logged, including access to PII. Users of the system (VA employees and contractors) are individually responsible for appropriate system usage. Misuse of information may result in employment termination or legal or civil penalties, as appropriate by law.

Additionally, audits are performed to ensure information is accessed and retrieved appropriately. New accounts added to VIEW CCM must be approved by a manager. VA and Salesforce have implemented required security and privacy controls for Federal information systems and organizations according to NIST SP 800-53 and VA Directive 6500.1, Risk Management Framework for VA Information Systems. All controls are per the approval of the Acting Assistant Secretary for information Technology [the VA Designated Accrediting Authority (DAA)].

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

- Name
- Social Security Number (Last four digits)
- Date of Birth (DoB)
- Mother’s Maiden Name
- Mailing Address
- Phone Number
- Fax Number
- Email Address
- Emergency Contact Information
- Financial Account Information
- Health Insurance Beneficiary Numbers
- Certificate/License numbers
- Vehicle License Plate Number
- Internet Protocol (IP) Address
- Current Medications
- Previous Medical Records
- Race/Ethnicity
- Tax Identification Number
- ICN
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.

Retention of Records is expected to be 75 years. The information is retained following the policies and schedules of VA’s Records Management Service and National Archives and Records Administration (NARA) in “Department of Veterans Affairs Records Control Schedule 101.” Record Control Schedule 10-1 can be found at the following link:


The NARA Records Disposition authority for VIEWS CCM is found at the following link:

Veterans Affairs Integrated Enterprise Workflow Solution (VIEWS) (archives.gov)

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.

VIEWS CCM 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 statutes, including the Federal Records Act (44 U.S.C. Chapters 21,
29, 31, 33) and NARA regulations (36 CFR Chapter XII Subchapter B). VIEWS CCM records are retained according to Record Control Schedule 10-1, Section 4 (Disposition of Records).


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.

### 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 deleted or changed by the VA. Data on backups is retained for 90 days until the backups are overwritten. Salesforce retains log data for one year. VA exports and retains data to meet VA/NARA retention requirements and disposes of the exported data at the end of the retention period.

When hard drives and backup tapes reach end of life, the media is sanitized based on Salesforce’s Media Disposal Policy. Hard drives are overwritten using a multi-pass write of complementary and random values. Successfully wiped disks or arrays will be returned to the vendor. Disks or arrays that fail during the wiping process will be retained and destroyed (in other words., degaussed, shredded or incinerated). Backup tapes are degaussed prior to disposal. Specifics on the sanitization process are described below.

Salesforce has an established process to sanitize production backup disks and hard drives prior to disposal, release from 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’s own Salesforce’s servers in Herndon, VA and Chicago, IL in the Salesforce Government Cloud server classification. This 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. Drives wiped successfully will be returned to the lessor. Drive that fail during the wiping process are retained in a locked container within the Salesforce data center facilities until onsite media destruction takes place. Leasing equipment allows Salesforce to use the latest equipment available from vendors.

Periodically, a third-party destruction vendor is brought onsite 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, SPI and more, are destroyed in accordance with the Department of Veterans’ Affairs Directive 6500.1, Electronic
When required, this data is deleted from their file location and then permanently removed from the deleted items or Recycle Bin. Magnetic media is wiped and sent out for destruction per VA Directive 6500.1. Digital media is shredded or sent out for destruction per VA Directive 6500.1. The OIT Chief/CIO is responsible for identifying and training OIT staff on VA media sanitization policy and procedures. The Information Security Officer (ISO) coordinates and audits this process and documents the audit on an annual basis to ensure compliance with National media sanitization policy.

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.

PII data is only stored in the production and staging environments. Access to these systems is protected using SSO technology to verify the user, and data access is provided based on permissions set up for that user. All other environments, including development and training, use lower-level servers that do not host PII data.

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.

Privacy Risk: Longer retention times within VIEWS CCM increase the risk that information can be compromised or breached.

Mitigation: VIEWS CCM adheres to the VA Record Control Schedules for each category or data it maintains. When the retention date is reached for a record, the VIEWS CCM team will carefully dispose of the data by the determined method as described in question 3.4. All electronic storage media used to store, process or access VA records will be disposed of in adherence with the latest version of VA Directive 6500.1, Electronic Media Sanitization.

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.
<table>
<thead>
<tr>
<th>Data Shared with Internal Organizations</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>List the Program Office or IT System information is shared/received with</strong></td>
</tr>
<tr>
<td>Active Directory Federated Service (ADFS)</td>
</tr>
<tr>
<td>Master Person Index (MPI)</td>
</tr>
<tr>
<td>IAM Access Services System (IAM ACS)</td>
</tr>
</tbody>
</table>
4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

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

**Privacy Risk:** Information may be shared with unauthorized VA personnel.

**Mitigation:** Safeguards, including employee security, privacy training and required reporting of suspicious activity, are implemented to ensure data is not sent to unauthorized VA employees. VIEWS CCM security measures include secure passwords, access on a need-to-know basis, Personal Identification Verification (PIV) cards, Personal Identification Numbers (PIN), encryption and access authorization.

### 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

<table>
<thead>
<tr>
<th>List External Program Office or IT System information is shared/received with</th>
<th>List the purpose of information being shared / received / transmitted with the specified program office or IT system</th>
<th>List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program or IT system</th>
<th>List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)</th>
<th>List the method of transmission and controls in place to secure data</th>
</tr>
</thead>
<tbody>
<tr>
<td>VA Salesforce Government Cloud Plus (SFGCP)</td>
<td>Case record retention</td>
<td>Name, SSN, Age, DoB, Gender, Address, Email Address, Previous Medical Records, Mother’s Maiden Name, Phone Number(s), Fax Number, Mailing Address Previous Mailing Address, Emergency Contact Information, Financial Account Information, Health Insurance Beneficiary Account Numbers, Certificate/License Numbers, Vehicle License Plate Number, IP Address, Current Medications, Previous Medical Records, Race/Ethnicity, Tax Identification Number, Medical Record Number, Other Unique Identifying Numbers</td>
<td>MOU/ISA 75VA001B/ 87 FR 36584</td>
<td>Connection between VIEWS CCM and the Salesforce Government Cloud Plus, which is a bidirectional Two-way Secure Socket Layer/ Transport Layer Security (SSL/TLS) encryption. The data between VIEWS CCM and Salesforce traverses through the Equinix (TIC) gateway.</td>
</tr>
</tbody>
</table>

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

**Privacy Risk:** With the exception of application data stored in Salesforce Government Cloud, data is not shared outside of the VA. If data is shared outside of the Department in the future, access controls will be implemented based on MOUs, contracts or agreements. If data is maintained outside of the VA, there is a risk that information may be accessed by an external organization or agency that does not have a need for or legal authority to access VA data.

**Mitigation:** VA has contracted Salesforce to deliver services that include maintaining VA data. A contract in place clearly articulates Salesforce’s roles and responsibilities. Authorized personnel access user-level data to provision and provide the Salesforce service. Access is controlled by authentication and is restricted to authorized individuals. Salesforce’s policies address the required security controls that must be followed in order to protect PII. Salesforce Development Platform Assessing will be connected to Equinix (the VA’s Trusted Internet Connection, otherwise known as TIC) for data transfer purposes.

Equinix will provide details of the security event, the potential risk to VA-owned sensitive information, and the actions that have been or are being taken to remediate the issue. Activities that will be reported include event type; date and time of event; user identification; workstation identification; success or failure of access attempts; and security actions taken by system administrators or security officers.

Equinix will also provide VA with a written closing action report once the security event or incident has been resolved. VA will follow this same notification process should a security event occur within the VA boundary involving Equinix’s provided data. Designated POCs will follow established incident response and reporting procedures, determine whether the incident warrants escalation and comply with established escalation requirements for responding to security incidents.

**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.

The Veteran provides user-level data that may contain PII for provisioning and providing the Salesforce service, and the Customer continues to have access to such information. VA does not otherwise share this information with Salesforce, except if required by law to do so. VA has sole ownership of the information and data located in Salesforce’s data center. VA is the only entity that has access to said data.

The following System of Records Notice (SORN) entries are related to VIEWS CCM: 75VA001B/87 FR 36584

The VA provides the public with two forms of notice that the system exists, including the Privacy Act of 1974 statement and the SORN. This PIA is a form of notice.

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

No personal data is collected directly from individuals. PIAs of other systems are available to be referenced as needed. The PIAs of the systems from which data was originally aggregated would cover the opportunity and right to provide or decline personal information requests. Both the SORN (75VA001B) and PIAs serve as a form of public notice.

6.3 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

This question is directed at whether an individual may provide consent for specific uses or the consent is given to cover all uses (current or potential) of his or her information. If specific consent is required, how would the individual consent to each use? This question is related to privacy control IP-1, Consent

No personal data is collected directly from individuals. PIAs of other systems are available to be referenced as needed. The PIAs of the systems from which data was originally aggregated would
cover the opportunity and right to provide or decline personal information requests. Both the SORN (75VA001B) and PIAs serve as a form of public notice.

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

Privacy Risk: VA employees, Veterans and individuals that submit information for Veterans will not know that applications built on the SFDP collect, maintain and/or disseminate PII and other SPI about them.

Mitigation: The VA ensures that it provides individuals with a notice of information collection and notice of the system’s existence through the methods discussed in question 6.1. The VA provides the public with two forms of notice that the system exists, as discussed in detail in question 6.1, including the Privacy Act of 1974 statement and the SORN.

Section 7. Access, Redress, and Correction
The following questions are directed at an individual’s ability to ensure the accuracy of the information collected about him or her.

7.1 What are the procedures that allow individuals to gain access to their information?

Cite any procedures or regulations your program has in place that allow access to information. These procedures, at a minimum, should include the agency’s FOIA/Privacy Act practices, but may also include additional access provisions. For example, if your program has a customer satisfaction unit, that information, along with phone and email contact information, should be listed in this section in addition to the agency’s procedures. See 5 CFR 294 and the VA FOIA Web page at http://www.foia.va.gov/ to obtain information about FOIA points of contact and information about agency FOIA processes.

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

If the system is not a Privacy Act system, please explain what procedures and regulations are in place that covers an individual gaining access to his or her information.
This question is related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.

No personal data is collected directly from individuals. Information in documents loaded to VIEWS CCM may contain PII gathered by users from other systems. PIAs of other systems are available to be referenced as needed. The PIA of the system from which the document creator originally captured the data would cover the information access procedures. The VIEWS CCM PIA will be published. Both the SORN (75VA001B) and PIAs serve as a form of public notice.

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.

No personal data is collected directly from individuals. Information in documents loaded to VIEWS CCM may contain PII gathered by users from other systems. PIAs of other systems are available to be referenced as needed. The PIA of the system from which the document creator originally captured the data would cover the information access procedures. The VIEWS CCM PIA will be published. Both the SORN (75VA001B) and PIAs serve as a form of public notice.

7.3 How are individuals notified of the procedures for correcting their information?

How are individuals made aware of the procedures for correcting his or her information? This may be through notice at collection or other similar means. This question is meant to address the risk that even if procedures exist to correct information, if an individual is not made fully aware of the existence of those procedures, then the benefits of the procedures are significantly weakened.

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

No personal data is collected directly from individuals. Information in documents loaded to VIEWS CCM may contain PII gathered by users from other systems. PIAs of other systems are available to be referenced as needed. The PIA of the system from which the document creator originally captured the data would cover the information access procedures. The VIEWS CCM PIA will be published. Both the SORN (75VA001B) and PIAs serve as a form of public notice.

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

Redress is the process by which an individual gains access to his or her records and seeks corrections or amendments to those records. Redress may be provided through the Privacy Act and
Freedom of Information Act (FOIA), and also by other processes specific to a program, system, or group of systems. This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

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

Operations managers and privileged users can update information on the Veteran’s behalf.

Individuals who discover that incorrect information was provided during intake can state that the documentation they are now providing supersedes that previously provided.

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.

Privacy Risk: Veterans whose records contain incorrect information may not receive notification of any changes. Furthermore, incorrect information in a Veteran’s record may result in improper identification.

Mitigation: No personal data is collected directly from individuals. Information in documents loaded to VIEWS CCM may contain PII gathered by users from other systems. PIAs of other systems are available to be referenced as needed. The PIA of the system from which the document creator originally captured the data would cover the information access procedures. The VIEWS CCM PIA will be published. Both the SORN (75VA001B) and PIAs serve as a form of public notice.

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.

User roles identity accessible information and applications. A user of the SFDP with appropriate permissions must sponsor other users to receive VIEWS CCM access. The sponsor will describe which applications the user needs to access, the user’s role and any applicable security caveats.

These roles will be governed by permission sets that allow field-level control of the information and data. Detailed user access policies and descriptions address prohibiting unauthorized disclosure and requirements for data breach notification, for payment of liquid damages in the event of a data breach, for security/privacy training and for signing the VA Rules of Behavior.

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 lead system administrator (SA), a contractor for VA, maintains governing authority over all SFDP environments. The SA maintains users, updates applications, introduces new functionality, governs deployment activity and ensures user operability. The SA is not a primary user of any application on the SFDP.

The SA will monitor and review contracts monthly. The system owner and Contracting Officer Representative (COR) is the individual to accept and amend any incoming or outgoing contracts involving SFDP VA Assessing.
Some VA contractors may have access to PII. All contractors have Non-Disclosure Agreements (NDAs) and have completed the appropriate background investigations for their respective roles. Contractors involved with system data migration must pass a Tier-4 background investigation.

Contractors who provide support to the system are required to complete annual VA Privacy and Information Security and Rules of Behavior training via the 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. After award, contractors are reviewed and provisioned into the Salesforce environment VA’s Digital Transformation Center (DTC) system administrators on an ad hoc basis, upon approval of the system owner.

**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.

Initial and annual Security Awareness Training includes security best practices, threat recognition, privacy, Health Insurance Portability and Accountability Act (HIPAA) compliance and policy requirements, and reporting obligations. Upon completion of training, personnel must complete a security and privacy quiz with a passing score. All required VA privacy training must be completed in TMS prior to the user being provisioned.

**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.
1. The Security Plan Status: Approved
2. The Security Plan Status Date: 26 Aug 2022
3. The Authorization Status: Approved
4. The Authorization Date: 30 Aug 2022
5. The Authorization Termination Date: 30 Aug 2023
6. The Risk Review Completion Date: N/A (Assess Only)
7. The FIPS 199 classification of the system (LOW/MODERATE/HIGH): Moderate

Section 9 – Technology Usage
The following questions are used to identify the technologies being used by the IT system or project.

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

*If so, Does the system have a FedRAMP provisional or agency authorization? If the system does 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.*

VIEWs CCM runs in the Salesforce Government Cloud Plus (SFGCP). Salesforce has been FedRAMP-certified for Platform as a Service (PaaS) and Software as a Service (SaaS) since 2014. All Salesforce Government Cloud Plus customers are on the same version, patch set and code base, minimizing security risk and lowering complexity. More than 40 other Federal agencies have issued an Authority To Operate (ATO) for solutions deployed on the Salesforce Government Cloud. In addition, security levels and permissions have been implemented to ensure workflow owners have access to the information they need while protecting sensitive data, such as PII and Protected Health Information (PHI).

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.*

The VA Salesforce contract establishes VA ownership rights of all data. The contract stipulates that the contractor shall not retain any copies of data, in full or in part, at the completion of the performance period. The data shall contain no proprietary elements that would preclude the VA from migrating the data to a different hosting environment or from using a different case management system in the future.
The Salesforce contract addresses the National Institute of Standards (NIST) 800-144 principle that states, “Organizations are ultimately accountable for the security and privacy of data held by a cloud provider on their behalf.”

If privacy-related data is disclosed, intentionally or unintentionally, VA would incur significant harm to its reputation, and violators may be held responsible with potential civil or criminal liabilities. In addition, VA could be compelled to provide credit monitoring services and other compensation to any customers who were thus harmed. Depending on the circumstances and root cause of a privacy disclosure incident, the cloud service provider’s reputation could be damaged.

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.

VIEWS CCM system objects contain: VA staff and system user identifiers, case emails, case queue ownership, case notes, case teams, associated contacts, contact roles and functional queue members. The MPI ICN is the external ID that is stored on the Contact object in Salesforce. This is the person record identifier between MPI and Salesforce. Additional SPI may include: Military Service History, Branch of Service, Place of Birth, Education History, Employment History, and Gender.

KnowWho contains biographical data on all MOC, Capitol Hill staffers, committees and caucuses. The data received is publicly available PII that may be sensitive.

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 has contracted Salesforce to deliver services that include maintaining VA data. A contract in place clearly articulates Salesforce’s roles and responsibilities. Authorized personnel access user-level data to provision and provide the Salesforce service. Access is controlled by authentication and is restricted to authorized individuals. Salesforce’s policies address the required security controls that must be followed in order to protect PII. Salesforce Development Platform Assessing will be connected to Equinix (the VA’s Trusted Internet Connection, otherwise known as TIC) for data transfer purposes.

Equinix will provide details of the security event, the potential risk to VA-owned sensitive information, and the actions that have been or are being taken to remediate the issue. Activities that will be reported include event type; date and time of event; user identification; workstation identification; success or failure of access attempts; and security actions taken by system administrators or security officers.

Equinix will also provide VA with a written closing action report once the security event or incident has been resolved. VA will follow this same notification process should a security event occur within the VA boundary involving Equinix’s provided data. Designated POCs will follow established incident response and reporting procedures, determine whether the incident warrants escalation and comply with established escalation requirements for responding to security incidents.

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).

VIEWS CCM does not utilize Robotics Process Automation (RPA).
### Section 10. References

#### Summary of Privacy Controls by Family

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

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

Gina A Siefert 273290
Digitally signed by Gina A Siefert
Date: 2022.10.06 15:18:53 -05'00'
Privacy Officer, Gina Siefert

JAMES BORING
Digitally signed by JAMES BORING
Date: 2022.10.06 13:39:51 -04'00'
Information System Security Officer, James Boring

Michael S. Domanski 326889
Digitally signed by Michael S. Domanski 326889
Date: 2022.10.06 13:23:24 -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).

The following System of Records Notice (SORN) entries are related to VIEWS CCM: 75VA001B/87 FR 36584

The VA provides the public with two forms of notice that the system exists, including the Privacy Act of 1974 statement and the SORN. This PIA is a form of notice.