Privacy Impact Assessment for the VA IT System called:

Salesforce Government Cloud Plus (SFGCP) Enterprise

Enterprise Project Management Office (EPMO)
Veterans Affairs Central Office-Enterprise (VACO)

Date PIA submitted for review:

8/15/2022

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Julie Drake	julie.drake@va.gov	202-632-8431
Information System Security Officer (ISSO)	James Boring	james.boring@va.gov	215-842-2000, Ext: 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 purpose of the Salesforce Government Cloud Plus – Enterprise (SFGCP – E) is to provide a trusted and secure service to the VA, VA contractors, and Federally Funded Research and Development Center (FFRDC) customers to quickly and securely deliver applications to meet customers' business needs. Customers can create business applications by tailoring applications built by Salesforce (i.e., the Salesforce Services) or by building their own custom applications on the Salesforce Lightning Platform. The SFGCP-E is both a Platform as a Service (PaaS) and Software as a Service (SaaS) model. The PaaS offering is available via the Salesforce Lightning Platform, which provides customers with a platform to develop their own customer applications entirely on-demand. The platform includes easy-to use, point-and-click customization tools to help customers create solutions for unique business requirements, without any programming experience. The SaaS offering is available via the Salesforce Services, which are applications built by Salesforce and available to customers for tailoring to meet their specific business needs. The Salesforce Services provide enterprise solutions for sales, partner relationship management, customer support, real-time collaboration, and other use cases determined by the customer. These services are identified in the Enterprise Mission Assurance Support Service (eMASS) as either major or minor applications hosted within the SFGCP-E authorization boundary. Each has their own specific PTAs completed as well as PIAs when applicable. The SFGCP-E information system is VA Controlled / non-VA Owned and Operated as it is owned and operated by Salesforce. The SFGCP-E is a dedicated portion of Salesforce's Platform as a Service (PaaS) and Software as a Service (SaaS) multi-tenant public cloud infrastructure, specifically isolated for use by the VA, VA contractors, and FFRDCs. The SFGCP-E is located in the Amazon Web Services (AWS) GovCloud (West) region. The authorization boundary includes applications and guest operating systems that reside on the AWS Infrastructure-as-a-Service (IaaS), and functions as part of that environment using associated AWS components and peripherals to secure the system from unauthorized access. It does not include the AWS services themselves, which are leveraged as part of the Amazon - AWS GovCloud FedRAMP authorization as of June 21, 2016.

Overview

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

- *The IT system name and the name of the program office that owns the IT system.*
- *The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission.*
- *Indicate the ownership or control of the IT system or project.*
- *The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.*
- *A general description of the information in the IT system and the purpose for collecting this information.*
- *Any information sharing conducted by the IT system. A general description of the modules and subsystems, where relevant, and their functions.*
- *Whether the system is operated in more than one site, and if so, a description of how use of the system and PII is maintained consistently in all sites and if the same controls are used across sites.*
- *A citation of the legal authority to operate the IT system.*

- *Whether the completion of this PIA will result in circumstances that require changes to business processes*
- *Whether the completion of this PIA could potentially result in technology changes*
- *If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval? If the system is using cloud technology, does the SORN for the system cover cloud usage or storage?*

• **The IT system name and the name of the program office that owns the IT system**: Salesforce Government Cloud Plus – Enterprise (SFGCP-E) owned in collaboration between Veterans Affairs Central Office (VACO) Information Technology Support Service's (ITSS), Access Management/VA Business Owners and Office of Information Technology (OIT).

• **The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission**: Salesforce is a Software-as-a-Service (SaaS) development environment that supports Veterans Affairs Central Office (VACO) Information Technology Support Service's (ITSS). Development and deployment of VA Salesforce application takes place in AWS. VA Salesforce is an enterprise-wide system. VA Salesforce System Administrators, and personnel delegated by the administrator, have access permissions that allow the user to access the App Setup. The App Setup contains options to customize a Salesforce Org and build, deploy, and manage applications. The App Setup allows authorized platform users to customize standard tabs and types of records; create applications and customize the customer's Salesforce Org using point--and--click tools, including managing call center settings, access and use Salesforce provided development tools to create applications and customize the customer's Salesforce Org, monitor the deployment of setup configurations, view installed packages from the AppExchange and control when critical updates are enabled on the organization.

- **Indicate the ownership or control of the IT system or project**: VA Controlled / non-VA Owned and Operated IS.

• **The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual**: VA Salesforce is collects, processes and retains information from Veterans or dependents, VA employees, and VA contractors. There are approximately 25,000 platform and community users but this number varies depending on the minor applications which are deployed and the usage of those minor applications. Program officials have identified the minimum PHI / PII data elements required to be collected and stored by Salesforce Government Cloud Plus – Enterprise (SFGCP-E) system. The data elements will be provided directly from the individual or other VA System using automation via application programming interfaces (APIs) to support specific VA business processes and the subset of the PII the VA is authorized to collect. The legal authority to use or collect SSNs is Executive Order 9397. The web pages that collect personal information will have a hyperlink to the Limited Privacy Policy that applies to the web page. VA's Privacy Policy can be found here. NOTE: The VA does not collect personal information unless the personal information is voluntary provided by the web user. The VA Privacy Act implementation rules are 38 CFR 1.575 - 38 CFR1.580 and can be found here.

• **A general description of the information in the IT system**: In accordance with the VA Office of Information and Technology (OIT) guidance, SFGCP-E is deployed in AWS being managed by VACO, ITSS. Multiple OIT teams, as well as VHA teams, utilize the shared resources within SFGCP-E to host their functionalities and tools for both staff and veteran facing minor applications. Additionally, SFGCP-E provides critical integration services back into the VA legacy systems to provide the interface for minor applications to work directly with the VA Systems.

• **Any information sharing conducted by the IT system**: A general description of the applications and subsystems, where relevant, and their functions: SFGCP-E consists of several key components called "applications". Each major and minor application is analyzed to determine if any elements of that application collects PII and each one has at a minimum its own PTA and a PIA when required. As new applications are added to the SFGCP-E environment, they will be required to have these documents completed before being authorized to operate.

• **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**: The primary site is the Amazon Web Services (AWS) GovCloud (West) region. The SFGCP-E consists of two virtual private clouds (VPCs) located in separate AWS Availability Zones (AZs): US-GOV-WEST-1A and US-GOV-WEST-1C. Each VPC represents all of the applications, computing resources, networking capabilities, and storage needed to support the SFGCP-E. To maximize availability, the SFGCP-E service is delivered using multiple AZs within the AWS GovCloud (West) region supporting primary and secondary replicated instances. The infrastructure utilizes carrier-class components designed to support millions of users. Extensive use of high-availability servers and network technologies, and a carrier-neutral network strategy, help to minimize the risk of single points of failure, and provide a highly resilient environment with maximum uptime and performance. The SFGCP-E services are configured to be N+1 redundant at a minimum, where N is the number of components of a given type needed for the service to operate, and +1 is the redundancy. The security controls protecting the PII data within VA Salesforce are documented in the approved SFGCP-E Authority to Operate (ATO). VA Salesforce is leveraging the security controls as part of the common services offered by AWS. The specific security controls leveraged by VA Salesforce, in addition to a detailed description of the SFGCP-E/Salesforce security boundaries, are documented in the VA SFGCP-E System Security Plan (SSP).

• **A citation of the legal authority to operate the IT system: The VA Salesforce cites the following legal authority references**: AUTHORITY FOR MAINTENANCE OF THE SYSTEM: 5 U.S.C. 301; 38 U.S.C. 501; 40 U.S.C. 11331; 44 U.S.C 3544; Executive Order 9397; Homeland Security Presidential Directive 12; Federal Information Processing Standard 201–1.

• **Whether the completion of this PIA will result in circumstances that require changes to business processes**: This PIA alone will not result in circumstances that require changes to business processes.

• **Whether the completion of this PIA could potentially result in technology changes**: The SFGCP-E and cloud hosting technologies were selected before this PIA was completed. PIA completion is not expected to 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?**: VA Salesforce is an existing system. However, the System Owner confirmed Salesforce is a technology and not a system of record. Individual minor applications built on the platform will require individual SORNs: In accordance with the VA Office of Information and Technology guidance, SFGCP-E is deployed in AWS while being managed by the VA. VA Salesforce leverages the FedRAMP certified HIGH security controls defined and implemented in the VA common services.

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)

VA Phone Number(s)
VA Email Address

PII Mapping of Components

SFGCP-E consists of several key components (databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by SFGCP-E 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
See Appendix A for a list of the 90 minor applications.					

SFGCP-E currently consists of over 90 key components (major and minor applications). Each application has been analyzed to determine if any elements of that application collect PII and each one will have at a minimum its own PTA and a PIA when required. As new applications are added to the SFGCP-E environment, they will be required to have these documents completed before being authorized to operate. All information regarding the use of PII is identified in each application's specific PTA/PIA. The number of applications added to SFGCP-E increases on a monthly average basis hence the reason to list "several" applications instead of a specific number.

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.

Current information retained, collected and processed is handled by the production applications in the VA Salesforce application. This information is retrieved from Veterans and internal VA IT systems in order to support the services provided to the platform and community users.

ADFS: All VA employees use their PIV to sign into SFGCP using ADFS. This IAM VA service checks the presented VA credentials from their PIV card against VA's Active Directory. If an employee is not a user in Active Directory, then the user will not have access to VA Salesforce application.

AccessVA: AccessVA is utilized in the credential validation process as well as assisting in the creation of a SSO external capability. Applications using IAM's AccessVA allow a Veteran to sign up, access, and use the application via accepted AccessVA credentials. Community/External users are authenticated to Salesforce using ID.me, with multi-factor authentication.

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.

Salesforce Government Cloud Plus – Enterprise is hosted in Salesforce Government Cloud Plus – FedRAMP cloud. SFGCP-E has two different methods of accessing the platform depending on the Org the application is hosted. The Orgs VA VET, VA MAIN, VALOB, VAEMPL, and VHA support OAuth with PIV to verify using OAuth to verify credential validation. When accessing the PM Org, Employees connect to utilizing SSO. When veterans or external users connect to the platform, they connect utilizing AccessVA. Access VA assisting in the creation of the SSO capability externally.

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.

VA Salesforce Government Cloud does not check for accuracy as the data is submitted by the user. If contact information is incorrect access will not be granted.

Components within the cloud have accuracy checks identified in the individual PTA/PIA.

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

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: 5 U.S.C. 301; 38 U.S.C. 501; 40 U.S.C. 11331; 44 U.S.C 3544; Executive Order 9397; Homeland Security Presidential Directive 12; Federal Information Processing Standard 201–1.

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: Salesforce Government Cloud Plus – Enterprise (SFGCP-E) platform has two internal VA connections to two other systems that transfers the information via HTTPs (Hypertext Transfer Protocol Secure). HTTP binds all traffic securely between the cloud and browser. Receiving the data from the other system transfers the risk to the other systems to ensure the data is accurate prior to transferring it to the SFGCP-E platform.

Mitigation: Application specific permissions are granted and assigned following the approval of a user permission request submitted by the application owner.

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.

ADFS: All VA employees use their PIV to sign into SFGCP using ADFS. This IAM VA service checks the presented VA credentials from their PIV card against VA's Active Directory. If an employee is not a user in Active Directory, then the user will not have access to VA Salesforce application.

AccessVA: AccessVA is utilized in the credential validation process as well as assisting in the creation of a SSO external capability. Applications using IAM's AccessVA allow a Veteran to sign up, access, and use the application via accepted AccessVA credentials. Community/External users are authenticated to Salesforce using ID.me, with multi-factor authentication.

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

SFGCP-E does not have tools to check the data received from the other two systems.

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?

This question is addressed in the application specific PIAs for any minor or major application hosted on SFGCP-E.

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

This question is addressed in the application specific PIAs for any minor or major application hosted on SFGCP-E.

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

This question is addressed in the application specific PIAs for any minor or major application hosted on SFGCP-E.

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.

ADFS: All VA employees use their PIV to sign into SFGCP using ADFS. This IAM VA service checks the presented VA credentials from their PIV card against VA's Active Directory. If an employee is not a user in Active Directory, then the user will not have access to VA Salesforce application.

AccessVA: AccessVA is utilized in the credential validation process as well as assisting in the creation of a SSO external capability. Applications using IAM's AccessVA allow a Veteran to sign up, access, and use the application via accepted AccessVA credentials. Community/External users are authenticated to Salesforce using ID.me, with multi-factor authentication.

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, VA e-mail address and VA telephone number.

3.2 How long is information retained?

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

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.

VA will retain PII for only as long as necessary to fulfill the specified purpose(s) and in accordance with a National Archives and Records Administration (NARA)-approved record retention schedule. OIT retains audit records for a defined time period to provide support for after-the-fact investigations of security incidents and to meet regulatory and VA information retention requirements. A minimum of 1 year or as documented in the NARA retention periods, HIPAA legislation (for VHA), or whichever is greater. Audit logs which describe a security breach must be maintained for 6 years (HIPAA requirement).

PII data retention period: Temporary; destroy when business use ceases. (GRS 4.2 item 140, DAA-GRS-2013-0007-0013).

Financial data retention period: Temporary; destroy when 3 years old, but longer retention is authorized if needed for business use. (GRS 1.1 item 001, DAA-GRS-2016-0013-0001).
Education data retention period: Temporary; destroy 7 years after the education activity is closed. (N1-015-11-4, Item 1 & 2).

NOTE: Not all major and minor applications associated with SFGCP will not retain data.

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.

This system 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. SFGCP records are retained according to Record Control Schedule 10-1 (reference: https://www.archives.gov/). Also see the General Record Schedule located here: https://www.archives.gov/files/records-mgmt/grs/grs04-2.pdf

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

SFGCP-E follows the OIT-OIS SOP MP-6-Electronic Media Sanitization procedures.

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

SFGCP-E does not use the data for research, testing or training.

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: If information is retained longer than specified, privacy information may be released to unauthorized individuals.

Mitigation: The risk associated with the length of time the data is retained is considered minimal. All data at rest within the SFGCP security boundary is encrypted in accordance with FIPS 140-2, as well as protected by FedRAMP certified "HIGH" security controls. Use of FedRAMP HIGH controls implemented under the FedRAMP ATO. Collectively, these controls within the SFGCP security boundary provide maximum protection to all VA Salesforce data. SFGCP only retains the required relevant information relevant as long as necessary to fulfill the specified purpose(s) and in accordance with a National Archives and Records Administration (NARA)-approved record retention schedule.

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***
Digital Transformation Center Integration Platform (DIP)	Digital Transformation Center Integration Platform	Name, Telephone Number, Email Address	Equinix Trusted Internet Connection (TIC) version 2.2. PII/PHI/SPI processed electronically via encryption.
Digital Veteran's Platform (DVP)	Digital Veteran's Platform (DVP)	Name, Telephone Number, Email Address	Equinix Trusted Internet Connection (TIC) version 2.2. PII/PHI/SPI processed electronically via encryption.

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: If appropriate safeguards are not in place, then Privacy information shared within the Department may result in unauthorized data access.

Mitigation: Release of PII to unauthorized individuals is prohibited by the Privacy standards mandated to all VA employees, affiliates, trainees, volunteers, and contractors. Both contractor and VA employees are required to take Privacy, Health Insurance Portability and Accountability Act (HIPAA), and information security training annually. Safeguards are implemented to ensure data is not sent to unauthorized VA employees, including employee security and privacy training, and required reporting of suspicious activity. Use of secure passwords, access on a "need to know" basis, Personal Identification Verification (PIV) Cards, Personal Identification Numbers (PIN), encryption, and access authorization are all measures that are utilized for the system. The VA Salesforce Business Owner defined the software product configuration requirements to customize data access needs for each role category, as well as limiting access within organizational boundaries.

Additionally, for some minor applications OGC privacy guidance outlines how the disclosure is consistent with the source system SORNs. Note, data is transmitted via secure connection to Salesforce. MVI keeps records of which users search for which individuals; Minor applications do not keep logs as this would require permanently storing data, which minor applications do not do, for privacy reasons.

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***
Salesforce Government Cloud Plus	Cloud Service Provider (CSP)	Name, Telephone Number, Email Address	"Salesforce Subscription Licenses, Maintenance	Site to site encrypted with Transmission

	Hybrid Solution		and Support", Contract Number: NNG15SD27B, Order Number: 36C10B9F0460.	Layer Security (TLS) 1.2

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: SFGCP-E is hosted in the Salesforce Government Cloud Plus -FedRAMP cloud. SFGCP-E does not have any interconnection outside the VA boundary. SFGCP-E does not need to have an ISA/MOU because the data is not shared outside of the boundary.

Mitigation: The Orgs VA VET, VA MAIN, VALOB, VAEMPL, and VHA support OAuth with PIV to verify using OAuth to verify credential validation. When accessing the PM Org, Employees connect to utilizing SSO. When veterans or external users connect to the platform, they connect utilizing AccessVA. Access VA assisting in the creation of the SSO capability externally.

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 Orgs VA VET, VA MAIN, VALOB, VAEMPL, and VHA support OAuth with PIV to verify using OAuth to verify credential validation. When accessing the PM Org, Employees connect to utilizing SSO. When veterans or external users connect to the platform, they connect utilizing AccessVA. Access VA assisting in the creation of the SSO capability externally.

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

Individuals/Veterans have the right to decline to provide their information; however, without providing the information cannot originate a specific minor application case record under the VA Salesforce Org.

Individuals may decline to provide information to community HMIS systems, as per each system's privacy policy. Individuals do not have the option to decline to provide information to the source VA systems.

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, the veterans cannot consent to pieces of their information. Individuals may decline to provide information to community HMIS systems for specific uses, as per each system's privacy policy. Individuals do not have the option to decline to provide information for specific uses to the source VA systems.

6.4 <u>PRIVACY IMPACT ASSESSMENT: Notice</u>

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:

<u>Principle of Transparency:</u> 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 members of the public may not know VA Salesforce Org. exists within the Department of Veterans Affairs.

Mitigation: The VA mitigates this risk by providing the public with one form of notice that the VA Salesforce Org exists; the Privacy Impact Assessment (PIA).

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.

As the system contains no information not represented in other systems, individuals would gain access to their information according to the means specified by each specific system (major and minor application) utilizing the SFGCP platform.

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.

For applications in which Salesforce is the SORN, users can open a help desk case which will notify the application business owner that information needs to be corrected. The SORN POC would also be contacted should the need arise to correct inaccurate or erroneous information.

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.

The Veteran or their beneficiaries are responsible for maintaining the accuracy of the data so that the Salesforce services can be provided. This information is collected for the purposes of contracting with or providing services to Veterans and is captured in the normal course of conducting business. The Veteran should correct or update the data as necessary during the intake process. The SORN POC would also be contacted should the need arise to correct inaccurate or erroneous information.

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

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

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

If the individual discovers that incorrect information was provided during intake and is wishing to obtain more information about access, redress, and record correction should contact the Department of Veterans Affairs regional office.

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: If individuals are not provided sufficient guidance regarding the access, redress, and correction of their data, then individuals could initiate adverse personnel actions against the Government.

Mitigation: By publishing this PIA, VA makes the public aware of methods for correcting their records. Because this system does not hold authoritative records long-term, it is unlikely individuals will feel the need to correct their information in this system.

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.

The SFGCP-E platform is accessible to both internal and external users who require logical access to VA information services. Account creation is managed and offered through VA via two factor authentication (2FA) Personal Identity Verification (PIV) card and/or AccessVA (SSOe). SFGCP-E entity will NOT allow users to perform any actions without appropriate identification and/or authentication. Internal/platform users must complete VA's OI&T On-boarding process and obtain a VA email address before a user account can be provisioned/permission in VA Salesforce platform.

Following IAM User Provisioning as implemented for VA Salesforce Community, user roles identify the information and application components a user can access. To receive access to VA Salesforce another system user with appropriate permissions must sponsor them. The sponsor will describe which functionality the user needs to access, the user's role, and any security caveats that apply to the user. These roles will be governed by permission sets that allow field level control of the information and data.

This information is documented in the user provisioning process with the Digital Transformation Center.

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 Salesforce Digital Transformation Center (DTC) contractor team supports the VA Salesforce production environment and as such has access to the VA Salesforce system and data contained therein. This includes PII and VA Sensitive Information. 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). Crystal Moultrie serves as the VA Contract Officer's Representative (COR) for the Salesforce DTC contract and Michael Domanski is the VA Salesforce System Owner. Mr. Domanski maintains governing authority over all VA Salesforce environments. The Salesforce DTC team maintains users, updates applications and components, introduces new functionality, governs deployment activities and ensures user operability. The Salesforce DTC members are not primary users VA Salesforce. Mr. Domanski monitors and reviews VA Salesforce related support contracts on a regular basis to ensure no gaps in support for the platform and community users. Developers do not have access to production PII.

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

VA offers privacy and security training. Each program or system may offer training specific to the program or system that touches on information handling procedures and sensitivity of information. Please describe how individuals who have access to PII are trained to handle it appropriately. This question is related to privacy control AR-5, Privacy Awareness and Training.

Personnel that will be accessing information systems must read and acknowledge their receipt and acceptance of the VA National Rules of Behavior (ROB) or VA Contractor's ROB prior to gaining access to any VA information system or sensitive information. The rules are included as part of the security awareness training that all personnel must complete via the VA's Talent Management System 2.0 (TMS). After the user's initial acceptance of the Rules, the user must re-affirm their acceptance annually as part of the privacy and security awareness training. Acceptance is obtained via electronic acknowledgment and is tracked through the TMS 2.0 system.

Community users are instructed to follow their organization's existing protocols regarding handling PII.

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: 29-Mar-2022
3. The Authorization Status: Authorization to Operate (ATO)
4. The Authorization Date: 30-Sep-2021
5. The Authorization Termination Date: 07-Aug-2023
6. The Risk Review Completion Date: 23-Sep-2021
7. The FIPS 199 classification of the system (HIGH).

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.

SalesForce Government Cloud Plus 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.

SFGCP is a Platform as a Service (PaaS).

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.

SFGCP-E ISO/ISSO/PO completes a Contract Security Checklist 6500.6 on all contracts to ensure that appropriate security and privacy requirements are included.

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.

As is true of most websites, Salesforce gathers certain information when individual users visit their websites. This information may include (i) identifiers, such as user ID, organization ID, username, email address and user type; (ii) commercial information; and (iii) internet activity information such as IP address (or proxy server information), device and application information, identification numbers, location, browser type, Internet service provider or mobile carrier, user interactions such as the pages and files viewed, website and webpage interactions including searches and other actions, operating system type and version, system configuration information, date and time stamps associated with usage and details of which of Salesforce products and product versions are being used.

In addition, Salesforce gathers certain information automatically as part of product usage and services ("Usage Data"). This information may include identifiers, commercial information, and internet activity information such as IP address (or proxy server), mobile device number, device and application identification numbers, location, browser type, Internet service provider or mobile carrier, the pages and files viewed, website and webpage interactions including searches and other actions taken, operating system type and version, system configuration information, date and time stamps associated with usage and details of which products and product versions are being used. In addition, Salesforce may use aggregate and de-identified Usage Data for other internal business purposes, such as to identify additional customer opportunities and to ensure that they are meeting the demands of customers and their users. Please note that this Usage Data is primarily used to identify the uniqueness of each user logging on (as opposed to specific individuals), apart from where it is strictly required to identify an individual for security purposes or as required as part of provision of the services to customers.

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.

This question is addressed in the application specific PIAs for any minor or major application hosted on SFGCP-E.

9.5 If the system is utilizing Robotics Process Automation (RPA), please describe the role of the bots.

Robotic Process Automation is the use of software scripts to perform tasks as an automated process that executes in parallel with or in place of human input. For example, will the automation move or touch PII/PHI information. RPA may also be referred to as "Bots" or Artificial Intelligence (AI).

The system does not utilize RPA.

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

Signature of Responsible Officials

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

JULIE C. DRAKE 969177

Digitally signed by JULIE C. DRAKE 969177
Date: 2022.08.23 07:20:00 -06'00'

Privacy Officer, Julie Drake

JAMES BORING

Digitally signed by JAMES BORING
Date: 2022.08.23 07:43:09 -04'00'

Information Systems Security Officer, James Boring

Michael S. Domanski 326889

Digitally signed by Michael S. Domanski 326889
Date: 2022.08.22 14:10:41 -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). Privacy, Policies, And Legal Information | Veterans Affairs

APPENDIX B

System contained in a cloud container or platform that are housed but do not share data with the container. Each of the listed systems on the table below are required to have their own individual PTA/PIA.

eMASS ID	System Name (list as in eMASS)
901	Nintex Drawloop - Enterprise
1097	MuleSoft Cloud - Enterprise
1462	TriageXpert Cloud - Enterprise
1467	Digital Automated Intelligence
1775	Salesforce - Academic Detailing
1776	Salesforce - Agile Accelerator
1777	Salesforce - Business Architecture Management Module
1778	Salesforce - Medical Disability Exam Quality
1797	Clinical Intake Prioritization
1798	Personnel Security Investigation Portal
1879	Salesforce - BioMed Recall Management
1880	Salesforce - Caregiver Records Management Application (CARMA)
1881	Salesforce - National Center for Healthcare Advancement and Partnerships (HAP)
1882	Salesforce - Veteran Relationship Management System (VRMS)
1883	Salesforce - Coaching
1884	Salesforce - Community Veterans Engagement Board (CVEB)
1885	Salesforce - Contract Manager
1887	Salesforce - Veterans Account Management System Debt Management Center (VAMS DMC)
1888	Salesforce - Education Development Management System
1889	Salesforce - Eforce Tool
1890	Salesforce - EMS Shift Clearing
1891	Salesforce - Environmental Program Site Review
1892	Salesforce - Extensible Assessment Manager ExAM
1893	Salesforce - ExAM4Inspections
1894	Salesforce - Integrated Ethics Web
1895	Salesforce - IT Intake
1896	Salesforce - Milestones PM+
1897	Salesforce - Mission Accountability Submission Tool
1898	Salesforce - Grants4Vets
1899	Salesforce - Office Finance Management Applications
1900	Salesforce - Office of Financial Management (OFM) Budget Formulation to Execution
1901	Salesforce - OFM Systems Workshop
1902	Salesforce - Quality Management System
1903	Salesforce - Quality Improvement Tracking Tool
1904	Salesforce - VA Prosthetics Order Vendor Interface & Delivery Tracking Solution (POVIDTS)
1905	Salesforce - VHA Integrity
1906	Salesforce - VA Integrated Enterprise Workflow Solution (VIEWS) Suspense
1907	Salesforce - VA Monthly Stipend Training Program
1908	Salesforce - Oversight and Accountability Reporting and Visualization Platform
1926	VA Health Connect Customer Relationship Management
1927	Salesforce -Emerging Technologies

1928	**Salesforce Insurance Disability Outreach**
1933	**Labor Pool Management Tool**
1934	**Occupational Health Record Keeping**
1935	**Salesforce - Veterans Engagement Reporting**
1936	**Salesforce - Learner Assessment Tool**
1937	**Salesforce - Citizen Developer Community**
1942	**Salesforce - Call Center Tracking**
1943	**Salesforce - OIT Ectropy**
1944	**Salesforce - Fiduciary Accounting Submission Tool (FAST)**
1945	**Salesforce - Government Accountability Office (GAO)**
1947	**Salesforce - New Office of Rural Health [ORH] Management and Analysis Database (NOMAD)**
1948	**Salesforce - Strategic Relationships**
1949	**Salesforce - VA Functional Organizational Manual (FOM)**
1950	**Salesforce - VA Help Desk Application**
1951	**Salesforce - VA Lighthouse API Support**
1952	**Salesforce - VA Office of Information Technology, Strategic Sourcing (VA OIT SS)**
1954	**Salesforce - Veteran Rapid Retraining Assistance Program**
1970	**National Center for Patient Safety Tools**
1975	**Salesforce - Status Query Response and Exchange System**
1976	**Salesforce - RPA Platform Management Tool**
1982	**VA National Telestroke Program**
1998	**Salesforce - Enterprise Management of Payments, Workload, and Reporting**
1999	**Salesforce - National Veterans Creative Arts (NVCA) Arts4Vets**
2008	**Salesforce - NVSPSE Registration4Vets**
2009	**Salesforce - Innovation Management**
2010	**Salesforce - TrackForce**
2015	**Veteran Affairs – Centralized Adjudication Background Investigation System**
2017	**Salesforce Dayton VAMC CRM**
2018	**Salesforce - Research Operations Command Center**
2021	**Clinical Trial Management Solution**
2022	**Salesforce - Attorney Fee Inventory Tracker**
2023	**Salesforce - VA Policy Library Pilot**
2035	**Salesforce - Whitehouse VA Hotline**
2037	**Salesforce - Workload and Time Reporting**
2039	**Salesforce - NCA Workload and Time Reporting System**
2042	**Salesforce - Consolidated Internship Solution**
2059	**Copado GovCloud-E**
2097	**Salesforce - Marketing Cloud – Veteran Experience Office**
2114	**Salesforce - Human Capital Service Center**
2115	**Salesforce - Telework accelerator**
2116	**Salesforce - DTC Product Portfolio Application**
2128	**Salesforce - Medical Disability Examination Office Invoice Validation Tool**
2129	**Salesforce - Virtual Customer Profile**
2136	**Salesforce - Health Information Technology (HIT) Subject Matter Expert (SME)**
2142	**Veterans Tracking Application 2.0**
2151	**Salesforce -Issue Management OIC Oversight and Accountability Reporting & Visualization Platform (OARVP)**