Privacy Impact Assessment for the VA IT System called:

Salesforce-Eforce Tool (SF-EFORCE)

Veteran Benefits Administration (VBA)
Education Program Management Office (EPMO)

eMASS ID #1889

Date PIA submitted for review:

October 17, 2024

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Renu Roy	Renu.Roy@va.gov	202-263-9119
Information System Security Officer (ISSO)	James Boring	James.Boring@va.gov	215-842-2000 x 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?".

Salesforce-Eforce Tool (SF-EFORCE) (also known as Salesforce - Government Cloud Eforce Module (SF-GCEM)) has multiple functions to support the streamlining of facility oversight in support of the maintenance of the G.I. Bill. The abstracts for the modules are:

SF-EFORCE (Approvals) – A School Certifying Official (SCO) makes a request to provide education benefits to Veterans and beneficiaries. The SCO submits the required documentation to the state approving agents (SAAs) for review and submittal to the VA via an electronic package of compiled required documents for the VA to review. The VA then approves the school or deems it Not Approvable. The SCOs may submit directly to the VA via a public URL. Submissions can include quarterly enrollment statistics, changes to SCO staffing (for access to VA systems) or other required reporting to remain in compliance with their Approval of programs.

SF-EFORCE (Compliance) – Tracks the training facilities to ensure they are complying with all regulations required to provide VBA benefits for Veterans who are receiving education benefits from VA. This was previously completed through a paper submission process. The VA user performing the compliance survey sends a request to the SCO for documentation. SCOs or SAAs can upload documents via a public URL (connected to a SF community) to the Salesforce record for VA review. Transferring the documents reduces exposure of PII via improperly encrypted email communication.

SF-EFORCE (Case/Feedback Tool Module) – IAW Executive Order 13607, Establishing Principles of Excellence for Educational Institutions Serving our Service Members, Veterans, Spouses, and Other Family Members, requires the establishment of a centralized way for students receiving Veteran educational benefits to provide feedback on their experiences with learning institutions. The purpose of the Feedback Tool is to provide a standardized method to submit feedback about an educational institution. Feedback can be positive or negative in nature. Negative feedback is tied to allegations that fall under the Principles of Excellence as outlined in the Executive Order. SF-EFORCE gives Education Service insight as to its beneficiaries' experiences.

SF-EFORCE (Referrals) – Only available to internal Eforce users. The module is used to document referrals to SAAs and track performance measures. Referrals are created by auditors to identify missing documentation or non-compliance with their Approval to provide benefits when surveying a school/training facility. The previous process was completed using paper, spreadsheets, and emails.

EFORCE (Reporting/Dashboards) – Tracks performance measures of SAAs, contract partners as identified in the annual cooperative agreement (contract). The tool helps VA users oversee and track multiple workflows in a simplified manner.

SF-EFORCE Edu Initiatives Community – Allows unauthenticated viewing and submission to apply for education opportunities that do not impact entitlement. The tool helps Veterans and their beneficiaries apply to receive new training opportunities without having to use their VA benefits.

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:

1 General Description

A. What is the IT system name and the name of the program office that owns the IT system?

Salesforce-Eforce Tool (SF-EFORCE); Education Program Management Office (EPMO) within Veterans Benefits Administration (VBA).

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

The information collected to manage data, workload and program management for the Education Service Oversight and Accountability team. All Education Liaison Representatives (ELRs), Education Compliance Survey Specialists (ECSSs), Education Case Managers are required to use SF-EFORCE to perform job duties relating to the oversight of Educational Training Institutes authorized to provide educational benefits to Veterans and their beneficiaries.

C. Who is the owner or control of the IT system or project?

VA Controlled / non-VA Owned and Operated

2. Information Collection and Sharing

D. What is the expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual?

The expected number of individuals whose information is stored in the system is 19,000. SF-EFORCE Compliance Module – VA User may elect to enter Student information being reviewed during the compliance audit. SF-EFORCE Case/Feedback Tool Module - Each client is either a Veteran or beneficiary, therefore there is a potential of up to 2 social security numbers (SSNs) associated with records. We average 130 cases/feedback each month in our complaint tracking module. We collect minimal PII when the Veteran or beneficiary submits cases/complaints relating to an Educational Training Institute. The information is collected through an online site that is accessed by the individual (often beneficiary) through www.VA.gov. The user accesses the SF-EFORCE form and enters the necessary information.

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

SF-EFORCE Compliance module – the VA user has the option to enter student records reviewed during the compliance survey in SF-EFORCE.

SF-EFORCE Case/Feedback module is a way of electronically tracking inquiries or feedback from Veterans and beneficiaries relating to the Education Training Institutes providing training under the VA GI Bill benefits. The purpose is to validate the user is a student and attempt to resolve the complaint.

F. What information sharing conducted by the IT system? A general description of the modules and subsystems, where relevant, and their functions.

SF-EFORCE uses an electronic MuleSoft integration to export data to Digital GI Bill (DGIB) Data Mart. DGIB is an up-to-date Education Business systems and operations platform. Personal and educational facility data stored in SF-EFORCE is shared with DGIB.

G. Is 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?

They system operates on one site which is accessed only by VA Employee users that have PIV card single sign on access.

3. Legal Authority and SORN

H. What is the citation of the legal authority to operate the IT system?

The SORN for SF-EFORCE is "Principles of Excellence Centralized Complaint System--VA" (170VA 22)

Link: https://www.govinfo.gov/content/pkg/FR-2022-05-02/pdf/2022-09377.pdf

As per the SORN, the legal authority for maintenance of the system is Executive Order (E.O.) 13607, ''Establishing Principles of Excellence for Educational Institutions Serving Service Members, Veterans, Spouses, and Other Family Members''.

Link: https://obamawhitehouse.archives.gov/the-press-office/2012/04/27/executive-order-establishing-principles-excellence-educational-instituti

I. 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 SORN, Department of Veterans Affairs, Privacy Act of 1974; System of Records "Principles of Excellence Centralized Complaint System--VA" (170VA 22/87 FR 25706) does not require amendment or revision. The SORN does cover cloud usage and storage.

4. System Changes

J. Will the completion of this PIA will result in circumstances that require changes to business processes?

Yes, business processes will be improved by:

1) Sharing SF-EFORCE data with Datamart. (internal to internal)

2) Public facing URL (Education file upload portal) which grants School Certifying Officials (SCOs) and VA contract partners (State Approving Agencies (SAA)) the ability to;

   a. upload requested documents to existing compliance survey records (eliminating PII exposure via email)
   b. submit documents and reports to remain compliant with their approval to provide education benefits.

K. Will the completion of this PIA could potentially result in technology changes?

SF-EFORCE will be enhanced to include an integration with MuleSoft to export SF-EFORCE data to DGIB.

Section 1. Characterization of the Information

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

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

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

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

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

- ☒ Name
- ☒ Social Security Number
- ☒ Date of Birth
- ☐ Mother's Maiden Name
- ☒ Personal Mailing Address
- ☒ Personal Phone Number(s)
- ☐ Personal Fax Number
- ☒ Personal Email Address
- ☐ Emergency Contact Information (Name, Phone Number, etc. of a different individual)
- ☐ Financial Information
- ☐ Health Insurance Beneficiary Numbers Account numbers
- ☐ Certificate/License numbers[1]
- ☐ Vehicle License Plate Number
- ☐ Internet Protocol (IP) Address Numbers
- ☐ Medications
- ☐ Medical Records
- ☐ Race/Ethnicity
- ☐ Tax Identification Number
- ☐ Medical Record Number
- ☐ Gender
- ☐ Integrated Control Number (ICN)
- ☒ Military History/Service Connection
- ☐ Next of Kin
- ☒ Other Data Elements (list below)

Other PII/PHI data elements: School Name, Work Mailing Address, Work Phone Number, Work Email Address

PII Mapping of Components (Servers/Database)

SF-EFORCE consists of 1 key component (servers/databases/instances/applications/software/application programming interfaces (API). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by SF-EFORCE and the reasons for the collection of the PII are in the table below.

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

Internal Components Table

Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
SF-EFORCE	Yes	Yes	Name, SSN, Date of Birth (DOB), Personal Mailing Address, Personal Phone Number, Personal Email Address, School Name, Military History/Service Connection, Work Mailing Address, Work Phone Number, Work Email Address	File Identification purposes, communication	Only authenticated VA users have access to the information.

1.2 What are the sources of the information in the system?
These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

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

SF-EFORCE Compliance module – student information is entered by VA user. Case/Feedback Tool module – information collected directly from individual as part of the public facing site or from other communication avenues (such as email) and entered by VA user.

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

The system does not rely on data from other sources.

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

SF-EFORCE is a source for approval, compliance, and complaint information about schools that provide education services to Veterans.

1.3 How is the information collected?

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

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

Information is not collected on a form. Information is collected electronically in the SF-EFORCE module.

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

Information is not collected on a form.

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

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

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

VA users validate student records manually looking up student records with VA internal resources. There is no automation done to validate the student records.

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

VA users are responsible for validating and correcting information. SF-EFORCE is not validating claimant SSN or other details for accuracy.

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

IAW Executive Order 13607, Establishing Principles of Excellence for Educational Institutions Serving our Service Members, Veterans, Spouses, and Other Family Members, requires the establishment of a centralized way for students receiving Veteran educational benefits to provide feedback on their experiences with learning institutions.

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. (*Work with your System ISSO to complete this section)*

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

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

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

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

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

Follow the format below when entering your risk assessment:

Privacy Risk: The internal VA Education users review Personally Identifiable Information (PII) to perform compliance audits or review Cases/Feedback Tool records. Due to the highly sensitive nature of this data, there is a risk that, if the data were accessed by an unauthorized individual or otherwise breached, serious personal, professional, or financial harm may result for the individuals affected.

Mitigation:

- The data secured in Salesforce Shield which utilizes FIPS 140-2 encrypted connection. Only authorized internal VA users login via single sign on to the application.
- SF-EFORCE adheres to information security requirements instituted by the VA Office of Information Technology (OIT).
- All employees with access to Veterans' information are required to complete the VA Privacy and Information Security Awareness training and Rules of Behavior annually.

Section 2. Uses of the Information

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

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

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

PII/PHI Data Element	Internal Use	External Use
Name	File Identification purposes	Not Used
Social Security Number (SSN)	File Identification purposes	Not Used
Date of Birth (DOB)	File Identification purposes	Not Used
Personal/Work Mailing Address	Communication	Not Used
Personal/Work Phone Number	Communication	Not Used
Personal/Work Email Address	Communication	Not Used
School Name	File Identification purposes	Not Used
Military History/Service Connection	File Identification purposes	Not Used

2.2 What types of tools are used to analyze data and what type of data may be produced?
These questions are related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information.

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

The data is not used for any analytical purposes. The data is used to determine Education Training Institutes compliance with MOU or determine the validity of Feedback provided.

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

The data is not used for any analytical purposes.

2.3 How is the information in the system secured?

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

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

The application utilizes Salesforce Shield protect adhering to FIPS 140-2 encrypted connection protests data at rest. SSN are encrypted within SF-EFORCE. Data in transit is protected using a MuleSoft integration that leverages Amazon Web Services (AWS) Red Shift.

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

Same as above, encryption within Salesforce. Additionally, SF-EFORCE stores the last 4 digits of SSNs.

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

Users accessing SF-EFORCE must be authenticated during login and granted access based on role. Additionally, PII in Salesforce applications is encrypted and each user that has access to the salesforce platform has to agree to the Privacy Information Security Agreement Rules of Behavior once a year that dictates how employees use/safeguard PII/PHI.

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information.

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

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

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

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

2.4a How is access to the PII determined?

Access to fields storing PII information is determined by the Role the user is setup in module. User Roles based on the job function determines the access to PII. Once Business owner, who is a VA Program Manager approves the user to access the system in a certain role that grants required Permissions to module. The module is configured with various Permission setting that decides who can access what. These settings are documented in Technical Design document which is reviewed by Digital

Transformation Center (DTC). Business owner is responsible for requesting User Setup based on the Role the User will be playing in the module. If there are any changes to Role (resource movement), Business reaches out to DTC to remove access for that specific user by submitting a User access request. Business Owner monitors all Users to ensure they have access only to what they are supposed to have. Business owner is responsible for safeguarding PII by utilizing features Salesforce provides – Permission sets and User activity logs.

2.4b Are criteria, procedures, controls, and responsibilities regarding access documented?

Yes, all requests for access to Salesforce are submitted by Management, Approved by System Administrator and completed by governing help desk, Digital Transformation Center Contractor.

2.4c Does access require manager approval?

Yes, a member of management must request access to the application for new or reactivation of accounts disabled due to inactivity of 45 days.

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

All electronic records with PII are stored within Salesforce for authorized users. All workflows are completely electronic.

2.4e Who is responsible for assuring safeguards for the PII?

Salesforce Encryption has been established and maintained since inception of the application.

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 (SSN)
Date of Birth (DOB)
Personal/Work Mailing Address
Personal/Work Phone Number
Personal/Work Email Address
School Name
Military History/Service Connection

3.2 How long is information retained?

In some cases, VA may choose to retain files in active status and archive them after a certain period of time. State active file retention periods, as well as archived records, in number of years, for the information and record types. For example, financial data held within your system may have a different retention period than medical records or education records held within your system, please be sure to list each of these retention periods. ***The VA records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented.*** *If the system is using cloud technology, will it be following the NARA approved retention length and schedule? This question is related to privacy control DM-2, Data Retention and Disposal.*

The information is retained following the schedules of VA's "Records Control Schedule VB-1 Part II, Central Office" found at the following link:
https://www.benefits.va.gov/warms/docs/regs/rcs_ii.doc

Records are maintained in the Readjustment Counseling Service (RCS) national computerized electronic client records will be maintained in the national computerized RCS Network (RCSNet) servers for 45 years after the last episode of service, after which time they will be destroyed.

The SORN provides the retention/destruction times set forth in the VBA Records Management, Records Control Schedule VB–1, Part 1, Section VII, as authorized by NARA.

The Privacy Act of 1974; System of Records policies and practices for retention and disposal states disposition of records is according to NARA guidelines.

3.3 Has the retention schedule been approved by the VA records office and the National Archives and Records Administration (NARA)?

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

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

Yes. SFGCP complies with all VA retention and disposal procedures specified in VA Handbook 6300 and VA Directive 6500. Records contained in the Salesforce FedRAMP cloud will be retained as long as the information is needed in accordance with a NARA-approved retention period. VA manages Federal records in accordance with NARA statues including the Federal Records Act (44 U.S.C. Chapters 21, 29, 31, 33) and NARA regulations (36 CFR Chapter XII Subchapter B). SFGCP records are retained according to VBA Records Control Schedule, VB-1, Part II & VBA Records Control Schedule, VB-1, Part I. DD

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

VBA records are governed by Records Control Schedule (RCS) VB-1, Part II Revised for VBA http://www.benefits.va.gov/WARMS/docs/admin20/rcs/part2/VB-1PartII.doc and by Records Control Schedule (RCS) VB-1, Part I

http://www.benefits.va.gov/WARMS/docs/admin20/rcs/part1/VB-1Part-I.doc Public Customer Service Operations Records, Item number: 1925.1. Disposition Authority, GRS 6.5, item 020. DAA-GRS-2017-0002-0001 (Records Control Schedule 10-1 (va.gov))

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

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

Data is moved to another backup server post retention period. VA's Salesforce Platform policy for data backup is applicable for this module. Electronic data and files of any type, including Protected Health Information (PHI), Sensitive Personal Information (SPI), Human Resources records, and more are destroyed in accordance with VA Directive 6500 VA Cybersecurity Program (February 24, 2021) and VA Handbook 6500.1 Electronic Media Sanitization. When required, this data is deleted from their file location and then permanently deleted from the deleted items or Recycle bin. Magnetic media is wiped and sent out for destruction. Digital media is shredded or sent out for destruction. https://www.va.gov/vapubs/search_action.cfm?dType=1

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

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

No training or testing is conducted using 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. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

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

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

Principle of Minimization: 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: Depending on the retention time, PII and sensitive information of the individual is at risk of exposure to unauthorized individuals. The information retained by the system is stored for reviewing and auditing of student records and Feedback submitted to VA relating to recipients of Education Benefits.

Mitigation: All data at rest in Salesforce platform is encrypted with Salesforce Shield which utilizes FIPS 140-2, in addition to being protected by FedRAMP security controls under the FedRAMP ATO.

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?

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***
DGIB DataMart	Consolidated data from SF-EFORCE to VA Education application under managed service.	Name, Social Security Number (SSN), Date of Birth (DOB), Personal/Work Mailing Address, Personal Phone Number, Personal Email Address, School Name, Military History/Service Connection	SQL to MuleSoft to AWS Red Shift by Gov Cloud.

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. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

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

Follow the format below:

Privacy Risk: There is a risk of information being shared with unauthorized VA personnel.

Mitigation: Safeguards are implemented including assignment of appropriate User Roles and Module access settings in Salesforce (Automated Controls) and Operational Processes (Manual Controls). All VA users must login using PIV card, SF-EFORCE PII is encrypted and the platform is protected with Salesforce Shield. Users access data on need-to-know-basis.

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.

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***
NA	NA	NA	NA	NA`

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

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

Discuss whether access controls have been implemented and whether audit logs are regularly reviewed to ensure appropriate sharing outside of the Department. For example, is there a Memorandum of Understanding (MOU), contract, or agreement in place with outside agencies or foreign governments.
Discuss how the sharing of information outside of the Department is compatible with the stated purpose and use of the original collection.
This question is related to privacy control AR-2, Privacy Impact and Risk Assessment, AR-3, Privacy Requirements for Contractors and Service Providers, and AR-4, Privacy Monitoring and Auditing

Follow the format below:

Privacy Risk: There is no external sharing.

Mitigation: There is no external sharing.

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 6.1 on the last page of the document. Also provide notice given to individuals by the source system (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?

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

6.1a 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, Notice of Privacy Practice provided to individuals for VHA systems. If notice was provided in the Federal Register, provide the citation.

Veterans and/or beneficiaries applying for Education benefits must complete an application, VA FORM 22-1990, MAR 2023. The aforementioned form includes the following Privacy Act Notice in the section labelled "Request to Opt Out of Information Sharing with Education Institutions".
Privacy Act Notice: The VA will not disclose information collected on this form to any source other than what has been authorized under the Privacy Act of 1974 or title 38, Code of Federal Regulations, section 1.576 for routine uses (e.g., VA sends educational forms or letters with a Veteran's identifying information to the Veteran's school or training establishment to (1) assist the Veteran in the completion of claims forms or (2) for the VA to obtain further information as may be necessary from the school for the VA to properly process the Veteran's education claim or to monitor his or her progress during training) as identified in the VA system of records, 58VA21/22/28, Compensation, Pension, Education, and Veteran Readiness and Employment Records - VA,

published in the Federal Register. Your response is required to obtain or retain education benefits. Giving us your SSN account information is voluntary. Refusal to provide your SSN by itself will not result in the denial of benefits. The VA will not deny an individual benefits for refusing to provide his or her SSN unless the disclosure of the SSN is required by a Federal Statute of law enacted before January 1, 1975, and still in effect. The requested information is considered relevant and necessary to determine the maximum benefits under the law. While you do not have to respond, VA cannot process your claim for education assistance unless the information is furnished as required by existing law (38 U.S.C. 3471). The responses you submit are considered confidential (38 U.S.C. 5701). Any information provided by applicants, recipients, and others may be subject to verification through computer matching programs with other agencies. VA FORM 22-1990, MAR 2023 (B) If you haven't selected a school or training establishment: Step 1: Mail the completed application to the VA Regional Processing Office for the state or region of your home address. See the addresses below for VA Regional Processing Offices. Step 2: Wait for VA to process your application and notify you of its decision concerning your eligibility for education benefits. Respondent Burden: We need this information to determine your eligibility for education benefits (38 U.S.C. 3471). Title 38, United States Code, allows us to ask for this information. We estimate that you will need an average of 15 minutes to review the instructions, find the information, and complete this form. VA cannot conduct or sponsor a collection of information unless a valid OMB control number is displayed. You are not required to respond to a collection of information if this number is not displayed. Valid OMB control numbers can be located on the OMB Internet Page at www.reginfo.gov/public/do/PRAMain. If desired, you can call 1-800-827-1000 to get information on where to send comments or suggestions about this form. The Harry W. Colmery Veterans Educational Assistance Act of 2017 (Public Law 115-48), also know as the "Forever GI Bill," requires the Department of Veterans Affairs (VA) to make available to educational institutions information about the amount of educational assistance to which a Veteran or other eligible individual is entitled. If you are eligible for the Post-9/11 GI Bill (Chapter 33), Montgomery GI Bill-Active Duty (Chapter 30), Montgomery GI Bill - Selected Reserve (Chapter 1606), or the Survivors' and Dependents Educational Assistance Program (DEA) (Chapter 35), you may elect to "opt-out" of these disclosures and have VA withhold this information instead. To request an opt-out, or for information about how to opt-out, please refer to our website at va.gov, or click https://www.va.gov/find-forms/ to complete the VA Form 22-0993, Request to Opt-Out of Information Sharing with Educational Institutions. REQUEST TO OPT OUT OF INFORMATION SHARING WITH EDUCATIONAL INSTITUTIONS WV WY APO / FPO AA FOREIGN SCHOOLS US VIRGIN ISLANDS NJ NY OH PA RI SD TN VA VT WI MD ME MI MN MO MT NC ND NE NH CO CT DC DE IA IL IN KS KY MA SERVES THE FOLLOWING STATES Eastern Region: VA Regional Office P.O. Box 4616 Buffalo, NY 14240-4616 APO / FPO AP GUAM PHILIPPINES MARIANA ISLANDS MS NM NV OK OR PR SC TX UT WA AK AL AR AZ CA FL GA HI ID LA SERVES THE FOLLOWING STATES Western Region: VA Regional Office P.O. Box 8888 Muskogee, OK 74402-8888 AMERICAN SAMOA PAGE

6.1b If notice was not provided, explain why. If it was provided, attach a copy of the current notice.

All users must complete an application with Privacy notice to establish a claim. A claim must be established before the VA can review student records or validate Feedback/complaints are submitted.

6.1c 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.

The Department of Veterans Affairs does provide public notice that the system does exist. This notice is provided in 2 ways:
1) The System of Record Notice (SORN) "Principles of Excellence Centralized Complaint System – VA" (170VA22) (March 30, 2022. This SORN can be found online at Link:
https://www.govinfo.gov/content/pkg/FR-2022-05-02/pdf/2022-09377.pdf.
2) This Privacy Impact Assessment (PIA) also serves as notice of the PITC Virtual VA system. As required by the eGovernment Act of 2002, Pub.L. 107–347 §208(b)(1)(B)(iii), the Department of Veterans Affairs "after completion of the [PIA] under clause (ii), make the privacy impact assessment] publicly available through the website of the agency, publication in the Federal Register.

Notice is also provided when individuals apply for education benefits using VA Forms: 22-1990, 22-1990e, 22-1990n, 22-1990t, 22-1999, 22-199b and 22-6553c.

6.2 Do individuals have the opportunity and right to decline to provide information? If so, is a penalty or denial of service attached?

This question is directed at whether the person from or about whom information is collected can decline to provide the information and if so, whether a penalty or denial of service is attached. This question is related to privacy control IP-1, Consent, IP-2, Individual Access, and IP-3, Redress.

Yes, Veterans and their families have the right to refuse to disclose their SSNs to VBA. The individual shall not be denied any right, benefit, or privilege provided by law because of refusal to disclose to VBA a SSN.

The Education Benefits Application includes Privacy Notice which provides instructions on how to decline by completing VA Form 22-0993, Request to Opt-Out of Information Sharing with Educational Institutions. In addition, the user is informed their application cannot be processed further.

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.

Individuals cannot consent to particular uses of the information they provide. Completion of the Education Benefits Application indicates consent to apply for education benefits. A link to the Privacy Act Statement is on the Education Benefits Application where it states Title 38, United States Code, allows VA to ask for information.

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. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

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

<u>Principle of Transparency:</u> Has sufficient notice been provided to the individual?

<u>Principle of Use Limitation:</u> 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: SF-EFORCE Feedback Tool – unauthenticated users have access to submit feedback on another's behalf. The Veteran or beneficiary may not be aware of a power of attorney (POA) or spouse submitting feedback without their direct knowledge. The risk is associated with the Veteran is not aware of the submittal.

Mitigation: The risk is mitigated by Veteran voluntary consent to the use of their information by applying for Education benefits, basic PII is a part of the data collection on the application. Contact information is provided on the online application which individuals/entities can use to submit complaints, comments, and requests for redress.

Additional mitigation is provided by making the System of Record Notices (SORN) and Privacy Impact Assessment (PIA) available for review online, as discussed in question 6.1 and the Overview section of this 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?

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

7.1a Cite any procedures or regulations your program has in place that allow access to information. These procedures, at a minimum, should include the agency's FOIA/Privacy Act practices, but may also include additional access provisions. ***For example, if your program has a customer satisfaction unit, that information, along with phone and email contact information, should be listed in this section in addition to the agency's procedures. See 5 CFR 294 and the VA FOIA Web page at http://www.foia.va.gov/ to obtain information about FOIA points of contact and information about agency FOIA processes.***

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

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

The application is not exempt from the Privacy Act.

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

The application is a Privacy Act application.

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.

The Privacy Act of 1974 affords Veterans the right to amend their records by submitting their request in writing. The request must be in writing and adequately describes the specific information the individual believes to be inaccurate, incomplete, irrelevant, or untimely and the reason for this belief. The written request needs to be mailed or delivered to the VA Regional Office that maintains the record. A request for amendment of information contained in a system of records must be delivered to the System Manager or designee for the concerned VBA system of records, and the facility Privacy Officer or designee, and needs to be date stamped; and filed Version appropriately. In reviewing requests to amend or correct records, the System Manager must be guided by the criteria set forth in VA regulation 38 CFR 1.579.

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

How are individuals made aware of the procedures for correcting his or her information? This may be through notice at collection or other similar means. This question is meant to address the risk that even if procedures exist to correct information, if an individual is not made fully aware of the existence of those procedures, then the benefits of the procedures are significantly weakened. This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

The procedure for correcting information is outline in this PIA, formal redress is provided. All information correction must be taken via the Amendment process.

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

Redress is the process by which an individual gains access to his or her records and seeks corrections or amendments to those records. Redress may be provided through the Privacy Act and Freedom of Information Act (FOIA), and also by other processes specific to a program, system, or group of systems. ***Example: Some projects allow users to directly access and correct/update their information online. This helps ensures data accuracy.***
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Formal redress is provided. All information correctio must be taken via the Amendment process. In addition, the individual may contact any Regional Office for guidance on how to gain access to his or her records and seek corrective action through the Amendment process.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

involved might change their behavior. *(Work with your System ISSO to complete all Privacy Risk questions inside the document this section).*

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: The individual may not be aware of how to access, redress or correct their information.

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

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?

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

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

As a part of the onboarding process, after the User is set up in the Active Directory, the Supervisor submits a request to the Education Service Operations team. They review, validate, and prepare the appropriate request with the DTC helpdesk, the team managing Salesforce Platform access. DTC reviews the details and grants appropriate access (ensuring the users are granted only the lowest privilege(s) needed to use SF-EFORCE.

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

Only VA employees have access to SF-EFORCE.

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

VA Education Service internal users are granted read/write access to data within SF-EFORCE based on their position. Users from VA OIG have read only access for data review purposes.

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.

Yes, SF-EFORCE contractors will have access to the system. Contractors will also be involved in the design, development, and maintenance of the system. All contractors who will utilize SF-EFORCE have signed NDAs. Contractors are bound by the same privacy and security procedures and requirements as VA employees.

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 who will be accessing information system must read and acknowledge their receipt and acceptance of the VA 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 which all personnel must complete via the VA's Talent Management System (TMS). After the ECC user's initial acceptance of the Rules, the user must re-affirm their acceptance annually as part of the security awareness training. Acceptance obtained through electronic acknowledgement is tracked through the TMS system. All VA employees and contractors must complete annual Privacy and Security training. This training includes, but is not limited to, the following TMS Courses: •VA Privacy and Information Security Awareness and Rules of Behavior •Privacy and Health Insurance Portability and Accountability Act (HIPPA).

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

Yes

8.4a If Yes, provide:

1. *The Security Plan Status*: Not Yet Approved
2. *The System Security Plan Status Date:* N/A
3. *The Authorization Status:* Authorization To Operate (ATO)
4. *The Authorization Date:* March 12, 2024
5. *The Authorization Termination Date:* March 12, 2026
6. *The Risk Review Completion Date:* N/A
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* Moderate

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

8.4b If No or In Process, provide your ***Initial Operating Capability (IOC) date.***
N/A

Section 9 – Technology Usage

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

9.1 Does the system use cloud technology? If so, what cloud model is being utilized?
If so, Does the system have a FedRAMP provisional or agency authorization? If the system does use cloud technology, but does not have FedRAMP authorization, explain how the Cloud Service Provider (CSP) solution was assessed and what FedRAMP documents and processes were used for the assessment in order to comply with VA Handbook 6517. Types of cloud models include: Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Commercial off the Shelf (COTS), Desktop as a Service (DaaS), Mobile Backend as a Service (MBaaS), Information Technology Management as a Service (ITMaaS). This question is related to privacy control UL-1, Information Sharing with Third Parties.

Yes, SF-EFORCE utilizes Salesforce Government Cloud Plus. Salesforce Government Cloud Plus is hosted in the AWS Government Cloud. The Salesforce Government Cloud Plus (SFGCP-E) is built on the underlying Salesforce Force.com that is hosted in a FedRAMP Certified FISMA High environment which is in the Amazon Web Services (AWS) GovCloud West. This software utilizes the PaaS Service of Salesforce Gov Cloud Plus. A MuleSoft AWS Red Shift integration allows dataflow to DGIB Data Mart.

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). (*Refer to question 3.3.2 of*

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

Service Provider: Contract entitled: "Salesforce Subscription Licenses, Maintenance and Support", Contract Number: NNG15SD27B, Order Number: 36C10B9F0460.

Yes, VA has full ownership of the PII that will be used by the SF-EFORCE module. Contract agreement "Salesforce Subscription Licenses, Maintenance and Support", Contract Number: NNG15SD27B, Order Number: 36C10B9F0460

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.

Yes, VA has full ownership of the ancillary data stored in the system.

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.

The cloud service provider does not collect ancillary data. VA has full authority over data stored in SF-EFORCE.

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).

SF-EFORCE 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.

RENU ROY

Digitally signed by RENU ROY
Date: 2024.11.12 09:51:08 -05'00'

Privacy Officer, Renu Roy

JAMES BORING

Digitally signed by JAMES BORING
Date: 2024.11.15 16:10:15 -05'00'

Information Systems Security Officer, James Boring

MICHAEL DOMANSKI

Digitally signed by MICHAEL DOMANSKI
Date: 2024.11.15 14:00:33 -05'00'

Information Systems 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; screen shot of a website collection privacy notice).

- Privacy, Policies, And Legal Information | Veterans Affairs

HELPFUL LINKS:

General Records Schedule
https://www.archives.gov/records-mgmt/grs.html

National Archives (Federal Records Management):
https://www.archives.gov/records-mgmt/grs

VA Publications:
https://www.va.gov/vapubs/

VA Privacy Service Privacy Hub:
https://dvagov.sharepoint.com/sites/OITPrivacyHub

Notice of Privacy Practice (NOPP):
VHA Notice of Privacy Practices
VHA Handbook 1605.04: Notice of Privacy Practices