Privacy Impact Assessment for the VA IT System called:

Salesforce – Mission Accountability Submission Tool (SF-MAST)

Veterans Benefits Administration

Office of Mission Support (OMS)

eMASS ID #: 1897

Date PIA submitted for review:

09/05/2024

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	*Chiquita Dixson*	*chiquita.dixson@va.gov*	202-632-8923
Information System Security Officer (ISSO)	*James Boring*	*james.boring@va.gov*	*215-842- 2000, Ext: 4613*
Information System Owner	*Mike Domanski*	*michael.domanski@va.gov*	*727-595-7291*

Abstract

The abstract provides the simplest explanation for "what does the system do?".

Salesforce – Mission Accountability Support Tool (MAST) is a workload tracker that tracks the type of service or facility requests for Support Services Division (SSD) for each Regional Office (RO). Each RO has an SSD that owns tasks that maintain the facility. Specific tasks may include requests for facilities maintenance (i.e., bathroom toilet not running, breakroom faucet not working, cubicle light needs to be replaced, housekeeping, or outside groundskeepers), requests for new/renewal PIV cards, building access, supplies, services, and/or equipment. Access is granted for users to input requests, where SSD Supervisors assign the work/task to a specific SSD employee to take care of the task. MAST helps to streamline and track work to completion. It also provides visibility and transparency to RO Leadership, District Leadership, and VA Central Office (VACO) Leadership, Under Secretary of Benefits (USB) Office, and Office of Financial
Management (OFM) on the amount of work that SSD personnel completes. This is managed by the Office of Mission Support (OMS).

The MAST Fleet Management functionality to be used by the RO to allow oversight of the management of the GSA motor pool (requesting a vehicle, scheduled/unscheduled maintenance, etc.), thereby tracking all work related to utilization, maintaining and servicing GSA vehicles. This enhancement will provide continuous streamlining of activities and enhanced oversight. This is managed by the Office of Mission Support (OMS).

The MAST - Enterprise Mail Management (EMM) module was designed to automate and consolidate VA's pre-existing manual database of mailroom expenditures that have been tracked via an Excel document known as the Smart Report for easy quarterly mail expenditure submissions. MAST – EMM is not being utilized by the field until further direction from VACO has been received. This module was designed, tested, and released to production without any input from the Office of Mission Support (OMS). Therefore, EMM is currently not managed by the Office of Mission Support.

The MAST-OMS module includes the ability to capture and track progress from beginning to end all Minor Construction (MC) projects to include the requirements, justification of requirements and projected/actual funding for the projects to provide increased visibility from VACO. Additional users will be added from each RO SSD for increased oversight, along with members of the USB and OFM Offices for awareness. This will be managed by the Office of Mission Support (OMS).

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 – Mission Accountability Submission Tool (SF-MAST) is controlled by Office of Mission Support (OMS) within the VBA. However, MAST-EMM is not managed by OMS personnel, nor was it designed with input from OMS.

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

Salesforce – Mission Accountability Support Tool (MAST) is a workload tracker that tracks the type of service or facility requests for Support Services Division (SSD) for each Regional Office (RO). Each RO has an SSD that owns tasks that maintain the facility. Specific tasks may include requests for facilities maintenance (i.e., bathroom toilet not running, breakroom faucet not working, cubicle light needs to be replaced, housekeeping, or outside groundskeepers), requests for new/renewal PIV cards, building access, supplies, services, and/or equipment. Access is granted for users to input requests, where SSD Supervisors assign the work/task to a specific SSD employee to take care of the task. MAST helps to streamline and track work to completion. It also provides visibility and transparency to RO Leadership, District Leadership, and VA Central Office (VACO) Leadership on the amount of work that SSD personnel completes.

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

Salesforce Government Cloud Plus (SFGCP) is a cloud platform, data in the platform is controlled by VA but non-VA Owned and Operated. Ownership rights to PII data should be covered in the Salesforce contract. Per NIST 800-144, it is understood that the organization (VA) is ultimately accountable for security and privacy of data held by Salesforce on our behalf.

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?

Potentially, thousands of individuals would be covered by the system and are typically VA employees. However, there may contain information on Veterans receiving equipment/supplies provided by the Veteran Readiness and Employment Services (VR&E) or Veterans participating in VA Loan Guaranty (LGY) programs.

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

Salesforce – Mission Accountability Support Tool (MAST) is a workload tracker that tracks the type of service or facility requests for Support Services Division (SSD) for each Regional Office (RO). Each Regional Office has an SSD that owns tasks that maintain the facility. Specific tasks include request for facility maintenance (i.e., bathroom toilet not running, breakroom faucet not working, or cubicle light out), supplies, equipment, and support from contracts to maintain the facility such as outside landscaping and building cleaning crew. Access is granted for users to input requests, where SSD Chiefs assign the work/task to a specific SSD employee to take care of the ask. Previously this was a sticky note or email request to the SSD team/Chief, and MAST streamlines and creates a tool to track work to completion as well as provide visibility and transparency for Regional Office (RO) leadership, District Leadership, and VA Central Office leadership. This includes employees who require PIV renewal or first-time issuance which is also a tasker that is owned by SSD. This is a workload tracker that will store tasks that are performed by Support Services

Division for employees at the local Regional Office (RO). The Cloud Computing is being used on the Salesforce Government Cloud Plus.

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

MAST-SSD streamlines and tracks mission support requests to completion within the Regional Office and provides visibility at the Central Office level. MAST is a standalone system with no interconnections.

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?*

Users are authenticated and allowed access into the tool using Single Sign On (SSO) two-factor authentication. User login and access is monitored by MAST. This system services nationwide and not a regional system. The controls are standardized nationwide. To gain access to MAST, users must use of Single Sign On (SSO) service using a Personal Identification Verification (PIV) card and associated credentials.

3. Legal Authority and SORN

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

The Privacy Act of 1974, set forth at 38 U.S.C. 501(a); 38 U.S.C. 73; 38 U.S.C. 75 SEC 4202; 5 U.S.C. Part III, Subparts D and E., Title 38, United States Code, section 7301(a), states the legal authority to utilize this information. The System of Records Notices (SORNs) applicable for the system are "Human Resources Information Systems Shared Service Center (HRIS SSC)—VA'' (171VA056A), "Case and Correspondence Management (CCM)–VA'' (75VA001B), and ''Veterans Health Information Systems and Technology Architecture (VistA) Records-VA'' (79VA10)

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?*

No, the SORN does not require an amendment. Yes, the SORN listed covers the cloud usage or storage; ''Veterans Health Information Systems and Technology Architecture (VistA) Records-VA'' (79VA10) https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28340.pdf.

4. System Changes

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

The completion of this PIA will not result in changes to business process.

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

No, the completion of this PIA will not result in technology changes.

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. It must also match the information provided in question 3.4 of the PTA.

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: VA Employee Identification Number, VA Email, VA Phone Number, Item Requested

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

PII Mapping of Components (Servers/Database)

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

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

Internal Components Table

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

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?

Information is collected directly from the individuals and input by VA employees and contractors into MAST application.

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 information is collected directly from the individual who are the source. No other sources of information are required.

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

The system is only utilized for tracking of request. No score card or analysis is created.

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 collected directly from the individuals and input by VA employees into MAST application.

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?

The information is not collected on a form and is not subject to the Paperwork Reduction Act.

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.

The information is collected directly from the individual who are the source which is a manual process at the discretion of functional leadership to determine if acceptable.

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?

No

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

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

The Privacy Act of 1974, as amended, 5 U.S.C. § 552a, establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies. The authority of

maintenance of the system listed in question 1.1 is under Title 38, United States Code, section 7301(a) and 323.

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: Employee information such as name, employee identification number, and employee identification number can be at risk of exposure.

Mitigation: The information exchange is through a MOU/ISA encrypted transmission. The data exchange will be through a site-to-site encryption having Transmission Layer Security. Salesforce Shield Product provides FIPS 140-2 certified encryption.

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
Veteran Name	Used as an identifier	N/A

Veteran File Number	Used as an identifier	N/A
Veteran Email	Secondary means of contact	N/A
Veteran Phone Number	Secondary means of contact	N/A
Veteran Address	Used as an identifier	N/A
PII/PHI Data Element	**Internal Use**	**External Use**
VA Employee Name	Used as an identifier	N/A
VA Email	Identify and contact the user	N/A
VA Phone Number	Identify and contact the user	N/A
Item/Task Requested	Identify and track services	N/A
VA Employee Identification Number	Identify the user	N/A
Escalation of Issues to Human Resources	Identify and track services	N/A
PII/PHI Data Element	**Internal Use**	**External Use**
VA Contractor Name	Identify the user	N/A
VA Email	Identify and contact the user	N/A
VA Phone Number	Identify and contact the user	N/A
Item Requested	To initiate and track services requested	N/A

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?

MAST-SSD and the Fleet module in MAST provides full transparency into the entire lifecycle of the request from:

- Initial submission to completion.
- Supports the needs of all user groups – ranging from SSD supervisors, SSD employees, and non-SSD requestors – by providing a one-stop-shop for all SSD requests.
- Information is logged and updated consistently, providing real-time snap shots of current state workflows.
- Provides reports and data analytics to assist in the overall management of all administrative functions necessary to support employees and the ROs' mission.
- Provides a central place for all dashboards and analytics.

The MAST-OMS module includes the ability to capture and track progress from beginning to end all Minor Construction (MC) projects to include the requirements, justification of requirements and projected/actual funding for the projects to provide increased visibility from VACO. Additional users will be added from each RO SSD for increased oversight, along with members of the USB and OFM Offices for awareness. This module is anticipated to be fully operational by the beginning of Fiscal Year 2026.

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.

Information in MAST is logged and updated consistently, providing real-time snapshots of current state workflows against the existing records. A new record created against VA employees or contractors are tracked against their respective names supporting the administrative functions of individual departments/ROs' mission.

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 data exchange will be through a site-to-site encryption having Transmission Layer Security. Salesforce Shield Product provides FIPS 140-2 certified encryption.

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

MAST does not collect, process, or retain SSN of individuals. Salesforce Shield Product provides FIPS 140-2 certified encryption.

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

MAST is an encrypted secure system and PII/PHI visibility is provided to users based on roles and profile settings.

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?

Role based hierarchy is applicable to the tool therefore based on designation the users can access the assigned content within the tool. Name and email address of VA employee utilizing the MAST tool will be seen while being utilized. Otherwise, no PII is being entered or accessed.
Users are provided access to PII only on a need-to-know basis to execute /facilitate a work tracking request within the MAST application. Typically, users are entering their own information within the request and have access to their own submitted requests. Profile based settings is applicable to the tool limiting the type of information accessed by individual users. Additionally, the SORN defines the use of the information and how the information is accessed, contained, and stored in the system.

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

Yes, controls are in place to ensure data is used and protected in accordance with legal requirements, VA policies, and VA's stated purpose for using the data. Controls include mandatory training completion for all employees, volunteers, and contractors. Additionally, audits are performed to ensure information is accessed and retrieved appropriately. VA and Salesforce have implemented required security and privacy controls for Federal information systems and organizations according to NIST SP 800-53 and VA Handbook 6500, Risk Management Framework for VA Information Systems. Per the approval of the Acting Assistant Secretary for Information Technology [the VA Authorizing Official (AO)]. VA Records Management Policy and the VA Rules of Behavior in Talent Management System (TMS) govern how Veterans' information is used, stored, and protected.

2.4c Does access require manager approval?

Yes, managers must approve an individual requesting access to the MAST application.

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

Leveraging the profile-based setting, users have limited access to PII information captured in the MAST application. It is not tracked, monitored, and recorded within the MAST module.

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

The ISO and ISSO are responsible for assuring the safeguards of the PII in the MAST tool. Accessibility to data is granted based on the permission sets and profile-based settings is applied

based on FedRAMP Salesforce Gov Cloud Plus platform. Account creation is managed and offered through VA via two factor authentication (2FA) Personal Identity Verification (PIV) card and/or Access VA. Single Sign On external (SSOe) is used to provide credential access to VA modules/communities residing in the Salesforce application, the determinant of access is organizational affiliation rather than personal identity. For some module(s) the required organizational e-mail confirmation and multi-factor authentication (MFA) will be enforced (IAL1), but no identity proofing (IAL2) and vice versa. The managers will reject any applications from individuals who do not work with them, do not require access, or are not using the correct e-mail address.

Section 3. Retention of Information

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 What information is retained?

*Identify and list all information collected from question 1.1 that is **retained** by the system. This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal*

The information retained in the MAST application are:

- **Veterans:** Name, File Number, Email, Phone Number, Address
- **VA Employees:** Name, VA Email, VA Phone Number, Item Requested, Employee Identification Number, Escalation of Issues to Human Resources
- **VA Contractors Information:** Name, VA Email, VA Phone Number, Item Requested

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.*

Currently application system records follow the default standard of sustained storage unless specific policies dictate the need for deviation.

RCS 10–1, Item 2000.2 Information Technology Operations and Maintenance Records destroy 3 years after agreement, control measures, procedures, project, activity, or when transaction is obsolete, completed, terminated or superseded, but longer retention is authorized if required for business use (DAA–GRS–2013–0005– 0004, item 020). RCS10–1, Item 2100.3 2100.3, System

Access Records destroy 6 years after password is altered or user account is terminated, but longer retention is authorized if required for business use (DAA–GRS–2013–0006– 0004, item 31).

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, the information is retained following the policies and schedules of VA's Records management Service and NARA in "Department of Veterans Affairs Records Control Schedule 10-1". Record Control Schedule 10-1 can be found at the following link:
https://www.va.gov/vhapublications/RCS10/rcs10-1.pdf

Additionally, the retention schedule for SFGCP is also applied to MAST.

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

Records will be maintained and disposed of in accordance with VA Directive 6300. VA will use NARA regulations (36 CFR 1234.6) for managing electronic records.

RCS 10–1, Item 2000.2 Information Technology Operations and Maintenance Records (DAA–GRS–2013–0005– 0004, item 020).

RCS10–1, Item 2100.3 2100.3, System Access Records (DAA–GRS–2013–0006– 0004, item 31).

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 the Record Control Schedule 10-1 Section 4 (Disposition of Records).

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.

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.

PII is not used for research, testing, and/or training. As a mitigation testing, training, and research is performed in non-PII containing development environments using sample data. As well, training materials are developed in the same manner.

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: Data being retained longer than needed poses a risk to PII being compromised.

Mitigation: Records are destroyed 3 years after agreement, control measures, procedures, project, activity, or when transaction is obsolete, completed, terminated, or superseded, but longer retention is authorized if required for business use.

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***
N/A	*N/A*	*N/A*	*N/A*

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 no to minimal risk.

Mitigation: N/A, No sharing of information to other systems.

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***	***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***	***List the method of transmission and the measures in place to secure data***

	specified program office or IT system		***permit external sharing (can be more than one)***	
N/A	*N/A*	*N/A*	*N/A*	*N/A*

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

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: N/A

Mitigation: N/A

Section 6. Notice

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

6.1 Was notice provided to the individual before collection of the information? If yes, please provide a copy of the notice as an Appendix-A 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.

The Department of Veterans Affairs does provide public notice that the system does exist. This notice is provided in three ways:

1. Information is entered into MAST by the user itself for tracking the status on each request to completion.
2. The SORNs defines the information collected from VA employees and VA Contractors, use of information, and how the information is accessed and stored. SORNs for the system are, "Human Resources Information Systems Shared Service Center (HRIS SSC)—VA''(171VA056A), "Case and Correspondence Management (CCM)–VA'' (75VA001B), and ''Veterans Health Information Systems and Technology Architecture (VistA) Records-VA'' (79VA10)
3. This Privacy Impact Assessment (PIA) also serves as a notice of the Salesforce – Mission Accountability Support Tracker (MAST).

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

Notice provided via VA Privacy Policy

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.

This is utilized by VA employees and VA contractors who enter the information into the MAST application. Since MAST access is granted by SSOe only, and all accounts must be approved and activated prior to account usage, all MAST account holders must abide by VA Privacy Policy and VA OIT Rules of Behavior.

Notice provided via VA Privacy Policy

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

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

No, individuals cannot decline to provide information. As minimum information (Name and EIN) is collected in order to submit and process the work tracking requests.

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

This question is directed at whether an individual may provide consent for specific uses, or the consent is given to cover all uses (current or potential) of his or her information. If specific consent

is required, how would the individual consent to each use? This question is related to privacy control IP-1, Consent.

The purpose of information collection within MAST is for work tracking and expenditures, and therefore specific consent request is not currently built into the application or required.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

Describe the potential risks associated with potentially insufficient notice and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your 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 Transparency: Has sufficient notice been provided to the individual?

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

Privacy Risk: The information is collected directly from the source who are the accessing and utilizing the MAST application. Risk is associated with the information retention in the MAST application. This is mitigated as stated below.

Mitigation: The VA mitigates this risk by providing the public with notice that the system exists, as discussed in detail in question 6.1. Also, SORNs applicable for the system aid to mitigate the risk of notice are, "Human Resources Information Systems Shared Service Center (HRIS SSC)—VA'' (171VA056A), "Case and Correspondence Management (CCM)–VA'' (75VA001B), and ''Veterans Health Information Systems and Technology Architecture (VistA) Records-VA'' (79VA10)

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.

Users are allowed to gain access to their own information including the capability to edit said information by accessing the MAST application.

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)?

MAST application is not exempt from 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?

Individual information captured in the tool are the users. All personnel whose official duties require access to the information are trained in the proper safeguarding and use of the information.

Per the SORNs, ‘‘Veterans Health Information Systems and Technology Architecture (VistA) Records-VA’’ (79VA10), access to records is granted by following way, Employees or representatives designated in writing seeking information regarding access to VA records may write, email, or call the VA office of employment. A request for access to records must contain the requester’s full name, address, telephone number, be signed by the requester, and describe the records sought in sufficient detail to enable VA personnel to locate them with a reasonable amount of effort.

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.

Users would correct their own information as they self-enter their own data to submit work tracking requests.

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.

Users are notified of procedures during training specifically developed for the application.

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.

Users can access and update their own information within the application.

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: Individuals information stored in the tool are the members who can access the MAST application. Risk is associated with the individuals being unaware on the process of accessing the information post their tenure with the VA.

Mitigation: The risk to access, redress, and correction to PII information captured in the MAST application through written request with substantial information for reason of access of the information. These requests are to be sent to the VA Office location of their employment for review and approval. Details of the access for records can be found in the SORNs, "Human Resources Information Systems Shared Service Center (HRIS SSC)—VA'' (171VA056A), "Case and Correspondence Management (CCM)–VA'' (75VA001B), and ''Veterans Health Information Systems and Technology Architecture (VistA) Records-VA'' (79VA10)

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?

Users must submit a user access request case to platform management and be formally provisioned for access to the application after being approved by predesignated approvers. Managers must approve the VA employees accessing/requiring to access the MAST application. The access to the application the manager/ sponsor should provide a description of the user needs, user's role, and security caveats that apply to the user. The roles will be governed by the permission sets that allow field level control of the information and data. Per VA Directive 6500, the Office of Information Technology (OIT) develops, disseminates, and reviews/updates a formal, documented policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; along with formal, documented procedures to facilitate the implementation of the control policy and associated controls.

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?

N/A, there are no other agencies outside of the VA employees and VA contractors that have access to the MAST application.

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.

MAST-SDD/Fleet Role (Manage by OMS Personnel):

MAST Supervisor: Can be an SSD Chief or SSD Supervisor at the Station/RO level.

- Drives strategic vision of an area through reporting

MAST Facility Manager: Manages facility object. Can only be a MAST Supervisor (but may be any employee assigned to a station's SSD).

- Creates and edits facilities within MAST that are assigned to a RO. Might be out based.

MAST Requester: Anyone. Sees only individual records. Can be a non-SSD employee or an SSD employee.

- Creates and submits a request in MAST for SSD personnel to take action on.

MAST Fleet SSD Manager: Manages facility's fleet vehicles. Can only be a MAST Supervisor (but may be any employee assigned to a station's SSD).

- Assigns, tracks, and maintains a stations fleet vehicles as required.

MAST SSD Requester: SSD employee (supervisory or non-supervisory).

- Responsible for submitting or completing incoming tasks for services and/or supplies.

MAST SSD Employee: SSD employee (supervisory or non-supervisory).

- Responsible for completing incoming tasks for services and/or supplies.

MAST Mail Tracking Employee: SSD employee (supervisory or non-supervisory).

- Tracks all incoming and outgoing mail and package quantities and costs.

MAST Fleet Requester: Anyone. Can be a non-SSD employee or an SSD employee.

- Submits requests for GSA/fleet vehicles.

MAST-OMS Role (Managed by OMS Personnel):

Regional Office (RO) Initiators: Can be an SSD Chief or Supervisor at the Station/RO level

- Submits a request in MAST-OMS for a project. Can create, read, and edit only for the RO that they're assigned to.

RO Directors: Can be a RO Director or Assistant Director

- Approves/rejects a request in MAST-OMS for a project. Can read, approve/return only for the RO that they're assigned to. Conditional RO view.

District Directors: Can be a District Director or Deputy District Director (or designee)

- Approves/rejects a request in MAST-OMS for a project. Can read, approve/return only for the district assigned. Conditional district view.

Office of Field Operations (OFO) Users: Designated OFO personnel

- Approves/rejects a request in MAST-OMS for a project. Can read, approve/return all. Conditional view all.

Office of Mission Support (OMS) Administrators (Admins): SCIP Manager, Lead Project Managers, and designated OMS administrative personnel

- Read, assign/return/re-assign as needed, view all, conditional edits as needed.

OMS Project Managers (PMs): OMS Project Managers or Lead PMs

- Read, submit/re-submit as needed, view all, conditional edits as needed.

OMS Facilities Director's Office (FDO) Users: OMS Facilities Directorate Director and/or Deputy Director

- Approves/rejects a request in MAST-OMS for a project. Can read, approve/return all.

OMS Budget Office (BO) Users: OMS Budget Officer and/or Budget Analyst

- Approves/rejects a request in MAST-OMS for a project. Can read, approve/return all.

OMS Assistant Deputy Director of Operations (ADDO) Users: OMS Assistant Deputy Director of Operations or designee

- Approves/rejects a request in MAST-OMS for a project. Can read, approve/return all.

OMS Executive Deputy Director of Operations (EDDO) Users: OMS Deputy Executive Director or designee

- Approves/rejects a request in MAST-OMS for a project. Can read, approve/return all.

OMS Executive Director of Operations (EDO) Users: OMS Executive Director or designee

- Approves/rejects a request in MAST-OMS for a project. Can read, approve/return all.

Office of Financial Management (OFM) Users: Designated OFM personnel

- Approves/rejects a request in MAST-OMS for a project. Can read, approve/return all. Conditional view all.

Office of External Relations (OER) Users: Personnel designated by OER office

- Approves/rejects a request in MAST-OMS for a project. Can read, approve/return all. Conditional view all.

Under Secretary for Benefits (USB) Users: Personnel designated by USB office

- Approves/rejects a request in MAST-OMS for a project. Can read, approve/return all. Conditional view all.

MAST Product Owner: Create, read, edit, view all. OMS Facilities Directorate employee(s) only.

FAC DIR Director, Deputy Director & MAST Manager

- Create, read, edit, submit/re-submit as needed, approve/return as needed, view all.

MAST-HR Role

(OMS does not have any authority or knowledge on the below listed roles that are highlighted in green, which are specific to MAST-HR. OMS is not involved in the development of the HR module in MAST and is unclear if this module will be released in the future.):
Requester: Anyone. Sees only individual records (can be VBA Employees, Supervisors, SSD Employees, Supervisors, admins, HR Liaison, HR Assistant, HR Specialist, HR Supervisor and OTM HR Specialists)

- Creates and submits a request

HRC Liaison: Sees at a station level. Can escalate to HRC (for that station). Can be OTM HR Specialists and HR Liaison

- A person that creates, reviews, assigns, completes or escalates HR requests

HRC Workflow Manager: Has ability to always read/edit all requests for all HRCs and at all the stations for his/her assigned HRC. Can be HR Supervisor and OTM HR Specialists

- A person that creates, reviews, assigns, completes HR requests. Can assign to HR Assistant and HR Specialist

HRC Employees: Has ability to read/edit and work on requests assigned to him/her at the station, and

- A person who can create, review, assign and complete HR requests. Can assign

MAST-EMM Role
(OMS does not have any authority or knowledge on the below listed roles that are highlighted in blue, which are specific to MAST-EMM. OMS was not involved in the development of the EMM module.):
EMM Initiator Group: At station level for VHA, VBA, or NCA and initiates mail expense tracking

- A person who can create expenditure tracking records.

EMM Approver Group: At a higher level than the initiator

- A person who can approve expenditure tracking records

EMM Read Only: Has ability to read only on all EMM activities

- A person who can read only on expenditure tracking

EMM Admin Group: Has ability to create/read/edit on all features of EMM

- A person who can create/read/edit on all activities for EMM

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, the Salesforce Digital Transformation Center (DTC) contractor team supports the VA Salesforce production environment and system integrators or developers working on MAST application have access to the development and production environment as required. 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). The Salesforce DTC team will maintain users, update

applications and components, introduce new functionality, govern deployment activities, and ensure user operability. The Salesforce DTC contracting team are not primary users of MAST application.

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.

General Training includes: VA Privacy and Information Security Awareness and Rules of Behavior, TMS 10203 - Privacy and Health Insurance Portability and Accountability Act (HIPPA), VA On-Boarding enterprise-wide training, and annual information security training. After the user's initial acceptance of the Rules, the user must reaffirm their acceptance annually as part of the privacy and security awareness training. Acceptance is obtained via electronic acknowledgment and is tracked through the TMS system.

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

8.4a If Yes, provide:

1. *The Security Plan Status:* Approved
2. *The System Security Plan Status Date:* 06/07/2023
3. *The Authorization Status:* Approved
4. *The Authorization Date:* 06/13/2023
5. *The Authorization Termination Date:* 06/13/2026
6. *The Risk Review Completion Date:* 06/13/2023
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.
Note: For systems utilizing the VA Enterprise Cloud (VAEC), no further responses are required after 9.1*. (Refer to question 3.3.1 of the PTA)*

Yes. This software application utilizes the Salesforce Government Cloud Plus Platform-as-a-Service (PaaS), which is built on the underlying Salesforce.com that is hosted in a FedRAMP-certified FISMA-High environment, which is in the Amazon Web Services (AWS) GovCloud West cloud.

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.*

Yes, VA has full ownership of the PII/PHI that will be shared through the Salesforce – Mission Accountability Support Tracker (MAST). Contract agreement "Salesforce Subscription Licenses, Maintenance and Support", Contract Number: NNG15SD27B.

9.3 Will the CSP collect any ancillary data and if so, who has ownership over the ancillary data?
Per NIST 800-144, cloud providers hold significant details about the accounts of cloud consumers that could be compromised and used in subsequent attacks. Ancillary data also involves information the cloud provider collects or produces about customer-related activity in the cloud. It includes data collected to meter and charge for consumption of resources, logs and audit trails, and other such metadata that is generated and accumulated within the cloud environment.
This question is related to privacy control DI-1, Data Quality.

The VA has the ownership over the ancillary data. The CSP (Cloud Service Provider) does not collect ancillary data.

9.4 NIST 800-144 states, "Organizations are ultimately accountable for the security and privacy of data held by a cloud provider on their behalf." Is this principle described in contracts with customers? Why or why not?
What are the roles and responsibilities involved between the organization and cloud provider, particularly with respect to managing risks and ensuring organizational requirements are met? This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.

VA has full authority over data stored in MAST.

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).

MAST 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**

ID	Privacy Controls
DI-1	Data Quality
DI-2	Data Integrity and Data Integrity Board
DM	**Data Minimization and Retention**
DM-1	Minimization of Personally Identifiable Information
DM-2	Data Retention and Disposal
DM-3	Minimization of PII Used in Testing, Training, and Research
IP	**Individual Participation and Redress**
IP-1	Consent
IP-2	Individual Access
IP-3	Redress
IP-4	Complaint Management
SE	**Security**
SE-1	Inventory of Personally Identifiable Information
SE-2	Privacy Incident Response
TR	**Transparency**
TR-1	Privacy Notice
TR-2	System of Records Notices and Privacy Act Statements
TR-3	Dissemination of Privacy Program Information
UL	**Use Limitation**
UL-1	Internal Use
UL-2	Information Sharing with Third Parties

Signature of Responsible Officials

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

Dixson, Chiquita

Digitally signed by Dixson, Chiquita
Date: 2024.11.19 07:08:14 -05'00'

Privacy Officer, Chiquita Dixson

JAMES BORING

Digitally signed by JAMES BORING
Date: 2024.11.26 09:18:27 -05'00'

Information System Security Officer, James Boring

MICHAEL DOMANSKI

Digitally signed by MICHAEL DOMANSKI
Date: 2024.11.25 10:10:36 -05'00'

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; screen shot of a website collection privacy notice).

The Department of Veterans Affairs does provide public notice that the system does exist. This notice is provided in three ways:

1. Information is entered into MAST by the user itself for tracking the status on each request to completion.
2. The SORNs defines the information collected from VA employees and VA Contractors, use of information, and how the information is accessed and stored. SORNs for the system are, "Human Resources Information Systems Shared Service Center (HRIS SSC)—VA''(171VA056A), "Case and Correspondence Management (CCM)–VA'' (75VA001B), and ''Veterans Health Information Systems and Technology Architecture (VistA) Records-VA'' (79VA10)
3. This Privacy Impact Assessment (PIA) also serves as a notice of the Salesforce – Mission Accountability Support Tracker (MAST).

Notice provided via VA Privacy Policy

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