Privacy Impact Assessment for the VA IT System called:

Smartsheet Gov -enterprise

VA Corporate Office

Board of Veterans Appeals

Date PIA submitted for review:

3/30/2023

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Tonya Facemire	Tonya.Facemire@va.gov	202-632-8423
Information System Security Officer (ISSO)	Alison Duncan	Alison.Duncan@va.gov	602-627-2823
Information System Owner	Aimee Barton	Aimee.Barton@va.gov	216-707-7726

Abstract

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

Smartsheet Gov -enterprise provides a cloud collaboration platform to enable users to plan, capture, manage, automate, and report on work while utilizing various collaboration features. The Smartsheet Gov -enterprise application provides a simple, intuitive interface that empowers business users to quickly configure, adapt, and improve their work processes to speed execution. Various features within the application include project tracking, smart grids, calendars, dashboards, cards, portals, forms, automations, import via Data Shuttle, and project portfolio management with the Control Center application.

Smartsheet Gov -enterprise projects provide essential tools for effective project management and empower teams to execute together with speed and accountability, driving to successful outcomes faster. Smart projects allow users to manage every aspect of complex projects, and visualize tasks in Gantt, card, and calendar views. Smart grids provide a unified, customized view of projects that keeps teams on task and on time to easily track multiple moving parts. Smart calendars keep teams in sync with an interactive, comprehensive view of all activities and critical timelines. Smart dashboards provide project owners and stakeholders a robust, real-time view into the status of top key performance indicators, critical trends, and summary reports. Smart cards give teams a more visual way to communicate and collaborate in Smartsheet Gov -enterprise with a powerful way to see, share, and act on projects together. Smart portals bring teams together and keep them on the same page with an easy-to-create and maintain centralized information portal. Smart forms empower business users to speed execution and foster innovation by making it easy to collect and act on data. Smart automations put simple and powerful work process automation rules to work in a matter of minutes.

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. The IT system name and the name of the program office that owns the IT system.

SmartSheet Gov -enterprise; Board of Veterans' Appeals

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

Project Management support across multiple Board of Veterans' Appeals Divisions to include: Human Resources, Program Management & Logistics, and Professional Development Division. Smartsheet Gov -enterprise will also be used throughout the Department of Veterans Affairs for similar functionality and purposes throughout different departments/programs.

C. *Indicate the ownership or control of the IT system or project.*

Board of Veterans Appeals, Office of Appellate Support, Program Management & Logistics Branch, Procurement Support Team

2. Information Collection and Sharing

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

The specific number of individuals whose information is stored in the system will change as more VA offices begin to utilize the Smartsheet Gov -enterprise Enterprise ATO. With respect to the Enterprise use case - 20 at any given time; we are gathering PII from New Employees to process their PIV sponsorships. Once we have filed the PIV Sponsorship request through GSA, the employee data is deleted from Smartsheet Gov -enterprise.

E. *A general description of the information in the IT system and the purpose for collecting this information.*

As noted above, the PII will be collected from newly hired employees as part of their onboarding process. The employee will manually input the requested data, which includes: Full Name, Mailing Address, Social Security Number, Date and Place of Birth, and personal email. The data will be used by an onboarding agent to sponsor the new employee through GSA. Once the sponsorship action is complete, the employee data will be deleted from Smartsheet Gov -enterprise. Additional use cases as part of this Enterprise system will have similar functionality in that PII will be input manually and used for project management/organizational purposes. Should additionally sites, offices, etc. choose to utilize Smartsheet's ability to store privacy data they will do so in alignment with the Program Offices goals and specific program management tactics.

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

No system-to-system sharing is anticipated.

G. *Whether the system is operated in more than one site, and if so, a description of how use of the system and PII is maintained consistently in all sites and if the same controls are used across sites.*

The system will be operated in more than one site per the change in Enterprise use. The system will be used and maintained in accordance with Smartsheets protection of all PII data and alignment with the Program Offices goals for use. Data access will be restricted to admin level users.

3. Legal Authority and SORN

H. *A citation of the legal authority to operate the IT system.*

OPM/GOVT-1 General Personnel Records (11-30-2015)
https://www.govinfo.gov/content/pkg/FR-2015-11-30/pdf/2015-30309.pdf

AUTHORITY FOR MAINTENCE OF THE SYSTEM INCLUDES THE FOLLOWING WITH ANY REVISIONS OR AMENDMENTS: 5 U.S.C. 1302, 2951, 3301, 3372, 4118, 8347, and Executive Orders 9397, as amended by 13479, 9830, and 12107.

When VA employee signs a legal contract to work at the VA, they have agreed to have their contact information collected. The Privacy Act of 1974, as amended, 5 U.S.C. & 552a, established 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.

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?*

SORN will cover cloud usage and is being updated currently.

D. System Changes

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

It will result in a timelier badging process for new Board of Veterans' Appeals employees. It will also result in better project management tracking and clearer communication of information.

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

No.

Section 1. Characterization of the Information

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

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

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

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

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

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

☒ Name
☒ Social Security Number
☒ Date of Birth
☐ Mother's Maiden Name
☒ Personal Mailing Address
☒ Personal Phone Number(s)
☐ Personal Fax Number
☒ Personal Email Address
☐ Emergency Contact Information (Name, Phone Number, etc. of a different individual)
☐ Financial Information

☐ Health Insurance Beneficiary Numbers Account numbers
☐ Certificate/License numbers*
☐ 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
Employee ID
Place of Birth (City and State)

PII Mapping of Components (Servers/Database)

Smartsheet Gov -enterprise consists of 1 key components (servers/databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by Smartsheet Gov -enterprise 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 the server names in the table. The first table of 3.9 in the PTA should be used to answer this question.

Internal Database Connections

Database Name of the information system collecting/storing PII	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
VA Employees – Manual Input from New Employee Information Request Form	No	No	First and Last Name, Email Addresses, Home Addresses, Full DOB, Full SSN, Employee ID, Phone Number, Place of Birth (City and State)	Data organization from manual paper entry	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?

The information is collected directly from the individual as part of the PIV Sponsorship process. This information will also only be collected manually per additional Smartsheet Gov -enterprise use cases.

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.

N/A

1.2c If the system creates information (for example, a score, analysis, or report), list the system as a source of information.

N/A

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?

PII will be collected directly from the individual through a Smartsheet Gov -enterprise form once this capability has been completed. As of right now the information is being collected via the new hire form documented in the table above.

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

The current process is a manual paper document that is utilized to gather the information. The new process will be that the form will be a digital, Smartsheet form-not an official VA form. Paper forms will not be used.

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.

Information is provided by the individual data owner. Once the PIV Sponsorship agent has manually completed the PIV Sponsorship process through GSA, the employee data record will be deleted from Smartsheet Gov -enterprise. Additional use cases may collect this information directly from the data owner as well. No integrations will directly occur.

1.4b If the system checks for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract.

N/A

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

OPM/GOVT-1 General Personnel Records (11-30-2015)
https://www.govinfo.gov/content/pkg/FR-2015-11-30/pdf/2015-30309.pdf

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

AUTHORITY FOR MAINTENCE OF THE SYSTEM INCLUDES THE FOLLOWING WITH ANY REVISIONS OR AMENDMENTS: 5 U.S.C. 1302, 2951, 3301, 3372, 4118, 8347, and Executive Orders 9397, as amended by 13479, 9830, and 12107.

When VA employee signs a legal contract to work at the VA, they have agreed to have their contact information collected. The Privacy Act of 1974, as amended, 5 U.S.C. & 552a, established 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.

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: When any amount of PII is utilized in a system there is a certain level of risk. That risk can be duplication, manipulation, etc.
The system collects, processes, and retains PII from employees. If this information was breached or accidentally disclosed to inappropriate parties or the public, it could result in personal harm to the individuals impacted and adverse negative effect to the VA.

Mitigation: Smartsheet is working towards higher approvals and authorizations to ensure PII data is protected and accounted for in the vendors authority to operate.
Data collected, processed, and retained will be protected in accordance with VA Handbook 6500 and FIPS 140-2 encryption and data in-transit protection standards. All systems and individuals with access to the system will be approved, authorized, and authenticated before access is granted. VA annual privacy and security training compliance will be enforced for all VA employees, contractors, and vendors.

Section 2. Uses of the Information

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

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

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

Each of the employee data points listed below are required by GSA to sponsor the employee for a PIV Badge-granting them access to VA information systems and physical facilities when appropriate. That is the sole purpose for collecting PII, and the record will be deleted once entered into the GSA portal. For additional use cases the tool will be used for project management and communication.

Name: Used for PIV Badge access
SSN: Used for PIV Badge access
Date of Birth: Used for PIV Badge access

Personal Mailing Address: Used for PIV Badge access
Personal Phone Number: Used for PIV Badge access
Personal Email Address: Used for PIV Badge access
Place of Birth (City and State): Used for PIV Badge access

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.

As a 'no view' SaaS provider, Smartsheet does not access, use, or analyze customer data in any way. In the case of a customer support request or any other type of user inquiry that requires engagement from Smartsheet personnel, by default Smartsheet personnel will not access customer data. If the specific user inquiry requires access to customer data, it will be done in a limited manner related to the user inquiry. No data will be created or manipulated.

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 information will be provided by newly hired employee for PIV sponsorship. Only the PIV Sponsorship Agent(s) will have access to the information to manually transfer it into the GSA PIV Sponsorship portal. Once that action is complete, the employee information will be deleted from Smartsheet. Additional use cases will ensure only system level admin users or authorized personnel gain access to privacy information. Specific admin level users will need access to the information to perform duties. If duties can be met without gaining access to privacy information they will not gain access.

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?

Smartsheet standards require AES 256-bit encryption of customer data-at-rest (server-side encryption) in its cloud environment, via FIPS 140-2 validated modules. Smartsheet encrypts all data in-transit. The Smartsheet platform requires HTTPS connections with TLS 1.2 and AES encryption.

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

SSNs will be protected in the same manner as any other data, per the data-at-rest and data-in-transit encryption methodologies described above.

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

Smartsheet Gov -enterprise aligns with OMB Memorandum M-0-15 with respect to its security policies, procedures, and solutions to protect all VA customer data, including 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?

Need to know across all use cases for Smartsheet Gov -enterprise. With regards to the enterprise use case the PII is being collected directly from the individual for a very specific purpose, PIV Sponsorship, and only the PIV Sponsorship Agents will have access to the data. Once the agents complete their sponsorship actions within the GSA portal, they will delete the individual’s PII from Smartsheet Gov -enterprise.

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

Yes; there is a New Employee Onboarding Standard Operating Procedure (SoP) that will be updated once permission is granted for entering PII into Smartsheet Gov -enterprise. With regards to additional use cases – a proper Enterprise Use of Smartsheet Gov -enterprise SOP will be drafted by the VA.

2.4c Does access require manager approval?

Yes; With regards to the enterprise use case an HR Manager will have to request access for any new PIV Sponsorship agents. With regards to other potential use cases systems should be put in place to ensure approvals are confirmed by senior managerial staff.

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

Capabilities to ensure only the appropriate individuals who have been granted access to the PII will be in place. Those that do not have proper permissions will not access the information.

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

As the SaaS provider of the Smartsheet Gov -enterprise service, Smartsheet provides the technical and product capability-based safeguards for any PII that may reside within the service. The VA will be responsible for all other safeguards for any PII that may reside within the service.

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*

Smartsheet retains active data (data not deleted or subject to account termination) during the life of the subscription agreement. In the event a sheet is deleted, the sheet can be recovered for up to 30 days from the trash unless deleted from the trash. In the event of account termination, the account Sysadmin will have 30 days to export content from the platform after which it will no longer be recoverable by end-users. Within 180 days, this data will be rendered unrecoverable. Should additional assistance be needed, Smartsheet professional services may be engaged to create an agreed upon export format for return of data to the customer. The process for the return of customer content is addressed in Smartsheet's contractual agreements. Smartsheet aligns data destruction procedures with NIST SP 800-88 Revision 1 recommendations.

Exact data elements will align with the specific use case, but must align with what is listed in the PTA, PIA and ATO boundary.

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.*

Smartsheet retains all data entered or uploaded into the application for the entirety of the license agreement. The VA mains full ownership of all its data, and as such at any time may delete, remove, archive data at any time; The Board of Veteran's Appeals will maintain individual PII only as long as it takes to complete PIV Sponsorship actions, which is currently a weeklong process.

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.
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

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

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: Current and former Federal employees as defined in 5 U.S.C. 2105. (Volunteers, grantees, and contract employees on whom the agency maintains records

AUTHORITY FOR MAINTENANCE OF THE SYSTEM INCLUDES THE FOLLOWING WITH ANY REVISIONS OR AMENDMENTS: 5 U.S.C. 1302, 2951, 3301, 3372, 4118, 8347, and Executive Orders 9397, as amended by 13478, 9830, and 12107.

General Records Schedule (GRS) 2.2 titled Employee Management Records. Linked below. https://www.archives.gov/files/records-mgmt/grs/grs-trs33-sch-only.pdf

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.

Smartsheet retains active data (data not deleted or subject to account termination) during the life of the account. In the event a sheet is deleted, the sheet can be recovered for up to 30 days from the trash unless deleted from the trash. In the event of account termination, the Sysadmin will have 30 days to export content from the platform after which it will no longer be recoverable by end-users. Within 180 days, this data will be rendered unrecoverable. The process for the return of customer content is addressed in Smartsheet's agreements. Smartsheet aligns data destruction procedures with NIST SP 800-88 Revision.**This question response requires a customer component as well.

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.

As a 'no view' SaaS provider, Smartsheet does not access, use, or analyze customer data in any way.

3.6 <u>PRIVACY IMPACT ASSESSMENT: Retention of information</u>

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: Information in Smartsheet Gov -enterprise is only retained for establishing retention periods of the records and will be deleted by the team after 180 days unless the VA needs use of the data for longer.

Mitigation: Data will be rendered unrecoverable after 180 days if the data is not necessary for VA's use within a specific use case, department, etc.

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: Risks associated with the sharing of this information within the Department center around permissions and inappropriate access. The internal sharing of data could result in disclosure of PII to unintended parties or recipients.

Mitigation: Proper standard operating procedures are being enacted for the specific enterprise use case and will be implemented for general use of the Smartsheet Gov -enterprise tool to

ensure PII is not at risk during use. System admin level users will be the individuals accessing the PII.
Access must be requested and only the access required by VA persons or processes acting on behalf of VA persons is to be requested or granted.

Section 5. External Sharing/Receiving and Disclosure

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

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

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

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

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

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

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

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

Data Shared with External Organizations

List External Program Office or IT System information is shared/received with	***List the purpose of information being shared / received / transmitted with the specified program***	***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***	***List the method of transmission and the measures in place to secure data***

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

5.2 <u>PRIVACY IMPACT ASSESSMENT: External sharing and disclosure</u>

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

Discuss whether access controls have been implemented and whether audit logs are regularly reviewed to ensure appropriate sharing outside of the Department. For example, is there a Memorandum Of Understanding (MOU), contract, or agreement in place with outside agencies or foreign governments.

Discuss how the sharing of information outside of the Department is compatible with the stated purpose and use of the original collection.

This question is related to privacy control AR-2, Privacy Impact and Risk Assessment, AR-3, Privacy Requirements for Contractors and Service Providers, and AR-4, Privacy Monitoring and Auditing

Follow the format below:

<u>Privacy Risk:</u> N/A - Information will not be shared outside of the department.

<u>Mitigation:</u> 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.

OPM/GOVT-1 General Personnel Records (11-30-2015) SORN AUTHORITY FOR MAINTENCE OF THE SYSTEM INCLUDES THE FOLLOWING WITH ANY REVISIONS OR AMENDMENTS: 5 U.S.C. 1302, 2951, 3301, 3372, 4118, 8347, and Executive Orders 9397, as amended by 13479, 9830, and 12107.

When VA employee signs a legal contract to work at the VA, they have agreed to have their contact information collected. The Privacy Act of 1974, as amended, 5 U.S.C. & 552a, established 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.

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

Please provide response here

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.

N/A

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.

In accordance with the SORN this information must be collected and cannot be declined.

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 records in this system are records of the OPM and must be provided to those OPM employees who have an official need or use for those records. Therefore, if an employing agency is asked by an OPM employee to access the records within this system, such a request must be honored.

NOTIFICATION PROCEDURE: Individuals wishing to inquire whether this system of records contains information about them should contact the appropriate OPM or employing agency office, as follows: a. Current Federal employees should contact the Personnel Officer or other responsible official (as designated by the employing agency), of the local agency installation at which employed regarding records in this system. b. Former Federal employees who want access to their Official Personnel Folders (OPF) should contact the National Personnel Records Center (Civilian), 111 Winnebago Street, St. Louis, Missouri 63118, regarding the records in this system. For other records

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: There is a potential risk (as with any SaaS solution) that the information can be misrepresented or altered.

Mitigation: When VA employees sign a legal contract with the VA they agree to have their contact information collected, which is mentioned in the appropriate SORN. Proper steps for mitigation include: restricting access to privacy information for only specific users, Smartsheet encryption and automatic deletion of data, proper Authority to Operate documentation, etc.

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.***

Individuals wishing to inquire whether this system of records contains information about them should contact the appropriate OPM or employing agency office, as follows: a. Current Federal employees should contact the Personnel Officer or other responsible official (as designated by the employing agency), of the local agency installation at which employed regarding records in this system. b. Former Federal employees who want access to their Official Personnel Folders (OPF) should contact the National Personnel Records Center (Civilian), 111 Winnebago Street, St. Louis, Missouri 63118, regarding the records in this system. For other records covered by the system notice, individuals should contact their former employing agency. Individuals must furnish the following information for their records to be located and identified: a. Full name. b. Date of birth. c. Social security number. d. Last employing agency (including duty station) and approximate date(s) of the employment (for former Federal employees). e. Signature.

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).

N/A

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.

N/A

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.

CONTESTING RECORD PROCEDURE: Current employees wishing to request amendment of their records should contact their current agency. Former employees should contact the system manager. Individuals must furnish the following information for their records to be located and identified. a. Full name(s). b. Date of birth. c. Social security number. d. Last employing agency (including duty station) and approximate date(s) of employment (for former Federal employees).

e. Signature. Individuals requesting amendment must also comply with the Office's Privacy Act regulations on verification of identity and amendment of records (5 CFR part 297).

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.

OPM/GOVT-1 General Personnel Records (11-30-2015) SORN CONTESTING RECORD PROCEDURE: Current employees wishing to request amendment of their records should contact their current agency. Former employees should contact the system manager. Individuals must furnish the following information for their records to be located and identified. a. Full name(s). b. Date of birth. c. Social security number. d. Last employing agency (including duty station) and approximate date(s) of employment (for former Federal employees). e. Signature. Individuals requesting amendment must also comply with the Office's Privacy Act regulations on verification of identity and amendment of records (5 CFR part 297).

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.

N/A

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 privacy risk for VA employees in regards to access centers more so here on denied access.

Mitigation: System administrators and the vendor (Smartsheet) will ensure only specific access is granted to individuals that need access to the information. A VA employee may be denied access to the Smartsheet Gov -enterprise solution if they are not deemed a required party, but they are able to request details and deletions of their information from the system if they feel is necessary. This would need to be done by the vendor and the system administrator.

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.

The Smartsheet application supports an RBAC model with respect to administration, where system administrators (i.e. SysAdmin) can manage higher privilege features of the account such as user administration or administration of sheet sharing. With respect to the sharing of sheets, Smartsheet operates on a discretionary access model for the purposes of sharing sheets and collaboration. By default, sheets are not accessible unless shared with a user either directly or in a workspace. For full details please review:- https://help.smartsheet.com/articles/520100-user-types and- https://help.smartsheet.com/learning-track/free-users/user-types-and-permissions

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?

As of right now no additional agencies or individuals besides the enterprise use case team will be utilizing or accessing PII. When that changes this document will be updated.

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.

Users that have access to PII information will be admin-level users. Others will have read access only permissions or will not be able to access PII.

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.

As of now no contractors will have access to the PII in the system. This may change with future use cases.

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.

N/A

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:* 14-Aug-2020
3. *The Authorization Status:* Authorization to Operate (ATO)
4. *The Authorization Date:* 08-Apr-2021
5. *The Authorization Termination Date:* 19-Nov-2023
6. *The Risk Review Completion Date:* 01-Apr-2021
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* Moderate Impact

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.***

Not Applicable / NA

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)*

Smartsheet Gov -enterprise is a cloud-based SaaS offering, possessing a FedRAMP Moderate authorization issued by the JAB (Joint Authorization Board). Accordingly, Smartsheet Gov - enterprise' FedRAMP documentation package (SSP, SAP, SAR, CIS, etc.) along with Continuous Monitoring (ConMon) reporting is available via the government's OMB MAX portal (https://max.gov).

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. The customer (VA) maintains full ownership of all their data maintained within Smartsheet Gov. Smartsheet does not maintain any ownership rights of customer data.** This question response requires a customer component as well. (contract number)

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. Like all CSP providing SaaS/PaaS/IaaS solutions, ancillary data in the form of metadata is also generated and maintained by the CSP, in this case Smartsheet Gov-enterprise. This data does not contain any customer specific application data, and is used purely to operate the cloud environment securely and efficiently. As such, this data is owned by Smartsheet. To reiterate, this does not include any form of customer specific data.

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

What are the roles and responsibilities involved between the organization and cloud provider, particularly with respect to managing risks and ensuring organizational requirements are met? This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.

Yes. These provisions and conditions are identified within the contract and user agreement.

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).

Not applicable.

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

ID	Privacy Controls
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 they provided in this Privacy Impact Assessment is true and accurate.

Tonya L. Facemire 234776

Digitally signed by Tonya L. Facemire 234776
Date: 2023.05.02 10:20:42 -04'00'

Privacy Officer, Tonya Facemire

Alison A. Duncan 542213

Digitally signed by Alison A. Duncan 542213
Date: 2023.05.02 07:38:28 -07'00'

Information System Security Officer, Alison Duncan

AIMEE BARTON

Digitally signed by AIMEE BARTON
Date: 2023.05.03 10:17:47 -04'00'

Information System Owner, Aimee Barton

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).

HELPFUL LINKS:

Record Control Schedules:

https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf

General Records Schedule 1.1: Financial Management and Reporting Records (FSC):

https://www.archives.gov/files/records-mgmt/grs/grs01-1.pdf

National Archives (Federal Records Management):

https://www.archives.gov/records-mgmt/grs

VHA Publications:

https://www.va.gov/vhapublications/publications.cfm?Pub=2

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