Privacy Impact Assessment for the VA IT System called:

Slack Assessing -E

VA Corporate Office (VACO)

Office of Information and Technology (OI&T)

eMASS ID: 1115

Date PIA submitted for review:

11/21/2023

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Lynn Olkowski	Lynn.Olkowski@va.gov	(202) 632-8405
Information System Security Officer (ISSO)	Mark McGee	James.mcgee5@va.gov	520-358-3237
Information System Owner	Thomas Adams	Thomas.Adams@va.gov	214-857-0760

Abstract

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

Slack is a chat client that provides a centralized way for teams to communicate between VA employees and external stakeholders, e.g., vendors, other federal agencies, community program partners, perspective VA employees and contractors, and academia. Slack integrates with DevOps tools such as PagerDuty, Prometheus, Slack, and Jira to enable fast conversations around events triggered by actions in other DevOps tools.

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?

Slack-e Assessing / Office of Information and Technology (OI&T)

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

Slack provides a centralized way for teams to communicate with external stakeholders such as other federal agencies, community partners, perspective new employees and contractors, and academia, similar to email. Slack is the collaboration hub, where the right people are always in the loop and key information is always at their fingertips. Teamwork in Slack happens online in channels, which make it possible to share, archive and search – keeping a team's tools and conversations organized, up-to-date and easy to find. With Slack, the information, conversations, and software teams use to get work done are all in one place, making it easier and faster to get things done. The Slack App Directory has over 1,500 apps that can be integrated out of the box, and the platform's open APIs enable almost any service to be custom integrated in Slack. With Slack, teams are better connected, and people can work together and collaborate as easily online as they do in person.

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

VA Controlled / non-VA Owned and Operated

2. Information Collection and Sharing

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

The expected number of individuals whose information is stored in the system is 5000. The typical client and affected individual are VA employees, VA product teams, new employees, new contractors supporting VA, federal employees of other federal agencies, VA contractors, external programs that have partnered with VA to provide services to Veterans, educational institutions collaborating with VA on Veteran programs and/or as part of research efforts.

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

VA Employee collection as part of communicating with new employees as part of onboarding process and/or reporting information related to availability for report to duty. Name and email are collected to authorize access to Slack.

Name, date of birth, email address, phone number, test results (COVID-19 tests), symptoms, occupational exposures, vaccination history.

VA Contractors collected to authorize access to Slack.
Name, email address

Members of Public/Individuals collected as part of communicating with new employees as part of onboarding process.

Name, Sex, Race, Weight, Height, Hair Color, Eye Color, Place of Birth, Home Address, Closest VA Facility, Mobile Number

Members of Public/Individuals in partnership with VA to support Veteran programs and/or research. Name and email address is collected to authorize access to Slack.

Clinical Trainees information collected to authorize access to Slack.
Name, email address

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

Slack Assessing-E (Slack-E) is a centralized communication platform for collaboration between project teams.VA employees and VA contractors use Slack to share information that is considered public. Slack is a chat client that provides a centralized way for teams to communicate, similar to email but much better. Slack integrates with Development and Operations (DevOps) tools such as PagerDuty, Prometheus, GitHub, Jira etc. to enable fast conversations around events triggered by actions in other DevOps tools.

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?

Slack is a centrally hosted web-based application that is operated as a single instance.

3. Legal Authority and SORN

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

Privacy Act of 1974; System of Records

Slack is covered under VA SORN #150VA10.

I. *If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval? If the system is using cloud technology, does the SORN for the system cover cloud usage or storage?*

The system is not in the process of being modified.

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 circumstances that require changes to business processes.

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

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: COVID-19 Tests, Symptoms, Occupational exposures, Vaccination History
Members of Public/Individuals collected as part of communicating with new employees as part of onboarding process: Name, Sex, Race, Weight, Height, Hair Color, Eye Color, Place of Birth, Home Address, Closest VA Facility, Mobile Number

Members of Public/Individuals in partnership with VA to support Veteran programs and/or research: Name and email address is collected to authorize access to Slack.

Clinical Trainees information collected to authorize access to Slack: Name, email address.

PII Mapping of Components (Servers/Database)

Slack-e Assessing consists of **2** 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 Slack-e Assessing 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	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

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

Interface (API) etc.) that contains PII/PHI					
Slack Database	**No**	**Yes**	VA Employees - Name, date of birth, email address, phone number, test results (COVID-19 tests), symptoms, occupational exposures, vaccination history VA Contractors - Name, email address Members of the Public/Individuals - Name, Sex, Race, Weight, Height, Hair Color, Eye Color, Place of Birth, Home Address, Closest VA Facility, Mobile Number Clinical Trainees - Name, email address	• For VA employees and VA contractors to share information. • New employee onboarding • Reporting information related to availability for report to duty	Encrypted with FIPS 199 compatible encryption mechanism
Slack Server	**Yes**	**No**	VA Employees - Name, date of birth, email address, phone number, test results (COVID-19 tests), symptoms, occupational exposures, vaccination history VA Contractors - Name, email address Members of the Public/Individuals - Name, Sex, Race, Weight, Height, Hair Color, Eye Color, Place of Birth, Home Address, Closest VA Facility, Mobile Number Clinical Trainees - Name, email address	• For VA employees and VA contractors to share information. • New employee onboarding • Reporting information related to availability for report to duty	Hypertext transfer protocol secure (HTTPS)/ Transport Layer Security (TLS) 1.2,

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?

All users provide their name and email address to gain access to Slack. In addition, authorized users will communicate with other users in Slack. Slack enables users that are provisioned access to the Veterans Affairs instance to communicate with all other provisioned users. Users are able to identify one another by searching for either the users first and last name or their Slack handle (a unique username specific to the Slack application for a given user). This communication happens in a variety of means: • Channels – either public (any user in the instance can join them) or private (only invited users can join them) where messages, files, and integrations can interact and enable workflows.• Direct messages – one to one format in which users can message other users on the Veterans Affairs instance without other users seeing their conversation.• Calls – Slack enables VOIP calling for users within the Veterans Affairs instance. New employees onboarding to VA or reporting their incapacitation for work will provide information in a private channel or direct message as instructed by the VA supervisor or program.

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.
Information is received from other systems as part of product/project management based on thresholds set for notification. The information from the other systems is used to notify product/project teams so appropriate action can be taken to maintain expected level of availability and operational response.

Enter Major Application name here.

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

The system doesn't create information.

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?

Users will access SaaS web application and communicate with other users directly into Slack. Other SaaS tools also communicate with Slack to provide notifications for product/project teams to take action, as needed, to maintain operationally stability.

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?
This system does not collect information on a form, therefore, not subjected to Paperwrok 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.

Information is checked for accuracy by the user that enters the information. Information provided from another system is checked for accuracy by the product/project team that is receiving the information for action.

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?

System does not check for accuracy by accessing a commercial aggregator.

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

Slack is provided under –Public Law 114-31; Veteran Information: Title 38, United States Code, Section 5107, Title 38, United States Code, Section 5106, and Title 38 United States Code 5701. Title 38, United States Code, section 81 11 (38 U.S.C. 5811 I), titled "Sharing of Department of Veterans Affairs and Department of Defense Health Care Resources. "Title 10, United States Code, section 1104 (10 U.S.C.5 1104), titled "Sharing of Resources with the Department of Veterans Affairs," which incorporates Title 31, United States Code, section 1535 (31 U.S.C. 51 535), titled "Agency Agreements," also known as the "Economy Act." E-government Act of 2002 (44 U.S.C. §208(b)). 38 United States Code 5706.

1.6 <u>PRIVACY IMPACT ASSESSMENT: Characterization of the information</u>
Consider the specific data elements collected and discuss the potential privacy risks and what steps, if any are currently being taken to mitigate those identified risks. (*Work with your System ISSO to complete this section)*

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

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

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

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

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

Follow the format below when entering your risk assessment:

Privacy Risk: The name and email address are entered in Slack by the Account Manager to create user account for accessing Slack. No other PII, no PHI and no sensitive information is collected by the Slack SaaS. Due to the sensitive nature of this data, there is a risk that, if the data were accessed by an unauthorized individual or otherwise breached, limited harm, or even identity theft may result in an embarrassment to the VA.

Mitigation: The name and email address of users is visible to users of Slack for communication and collaboration. Information that should only be seen by designated individuals is communicated in private channels or by direct message to limit who can access and view information.

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
VA employees/Contractors/ Clinical Trainees and Members of the public - Name and Email address	File Identification purposes	Not used
Members of Public/Individuals: Name, Sex, Race, Weight, Height, Hair Color, Eye Color, Place of Birth, Home Address,	Collected as part of as part of new employee onboarding process.	Not used

Closest VA Facility, Mobile Number		
VA Employees - Name, date of birth, phone number, test results (COVID-19 tests), symptoms, occupational exposures, vaccination history	For report information related to availability to work or report to duty.	Not used

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

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

This system does not process or analyze the data submitted. The data provided is used by project teams to communicate and collaborate, similar to email but more efficient.

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.

This system does not process or analyze the data submitted. The data provided is used by project teams to communicate and collaborate more efficiently than using email.

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?

Secure socket layer is used to encrypt data in transit and at rest.

2.3b If the system is collecting, processing, or retaining Social Security Numbers, are there additional protections in place to protect SSNs?
This system does not collect, process, or retain Social Security Numbers

2.3c How is PII/PHI safeguarded in accordance with OMB Memorandum M-06-15?
VA Privacy Service in conjunction with the Senior Agency Official for Privacy (SAOP), the Privacy Compliance Assurance Office, and the Office of Enterprise Risk Management (ERM) are responsible for monitoring and auditing privacy controls continuously.

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?

All users have access to name and email address of other users for the purpose of communicating and collaborating.

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

Yes

2.4c Does access require manager approval?

Users can be invited to join Slack for communicating and collaborating. Approval for access is limited to System Administrators with role of workspace owner or workspace administrator.

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

User activities in the system are saved and available for review.

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

Users are responsible for adhering to VA policies and rules of behavior for safeguarding PII.

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

All data listed in section 1.1 is retained as part of creating user account for accessing Slack. The system retains information entered by Slack Account Manager. The information collected is the user's name and email address. Slack also retains communications entered by users.

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.*

Slack will keep VA data for as long as VA is a paying customer, backing up the data in accordance with FedRAMP and NARA requirements. In this specific context, it means that they are able to reconstitute/provide the data to VA in the event they needed it for the term that the VA is a customer and have the appropriate backup configurations to ensure this data is available in the event of a disaster. In the event that VA were to leave Slack, Slack would provide VA with ALL VA data and then the data would be deleted from our system within 14 days, thus relinquishing our responsibility of storing/curating that data.

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, In Slack information is retained for 75 years after the last record update. This retention period is required by the Department of Veterans Affairs Record Control Schedule 10-1, Records Control Schedule 10-1 (va.gov)

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

Retention and Disposal: The records must be disposed of in accordance with the records retention standards authorized by the National Archives and Records Administration General Records Schedule 14, published in the Veterans Health Administration Records Control Schedule 10–1, Records Control Schedule 10-1 rcs10-1.pdf (va.gov)

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

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

Slack is not used for research, testing or training. Employee name and email is used for intended purposes only which is communication and collaboration. Initial privacy training is required for new employees and contractors, and at least annually thereafter via the VA OIT Talent Management System (TMS). VA privacy awareness training program commences with the VA OIT TMS training, VA Privacy Information Security Awareness and Rules of Behavior (ROB), number 10176. Following the training, all information system users will be able to identify the types of information that must be carefully handled to protect privacy; recognize the required information security practices, legal requirements, and consequences and penalties for non-compliance; and explain how to report.

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: Records must be maintained to be accurate, relevant, timely and complete. The risk to maintaining data within Slack for a longer time period than what is needed or required is that the longer information is kept, the greater the risk that information will be compromised, unintentionally released, or breached.

Mitigation: Access to the system is governed by a need to know. All those with access have been trained in Privacy and Information Security. Slack is housed in a secure FedRAMP authorized Cloud.

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			

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 are no internal sharing of data

Mitigation: There are no internal sharing of data

Section 5. External Sharing/Receiving and Disclosure

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

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

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

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

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

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

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

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

Data Shared with External Organizations

List External Program Office or IT System information is shared/received with	***List the purpose of information being shared / received / transmitted with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program or IT system***	***List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)***	***List the method of transmission and the measures in place to secure data***
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: There is no external sharing of data

Mitigation: There is no external sharing of data

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.
VA SORN #150VA10 Enterprise Identity and Demographics Records-VA
2023-24193.pdf (govinfo.gov)..

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

VA SORN #150VA10 Enterprise Identity and Demographics Records-VA.
2023-24193.pdf (govinfo.gov)..

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.

Users access to the system is optional within the VA. If a user decides to create an account, the user will be asked to enter in their name and e mail. After this point users have communication with the VA team and can request information on how their PII is used and users have an option whether to provide or not provide this information requested. VA SORN #150VA10 Enterprise Identity and Demographics Records-VA2023-24193.pdf (govinfo.gov)..

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.
Users access to the system is optional within the VA. If a user decides to create an account, the user will be asked to enter in their name and e mail. After this point users have communication with the VA team and can request information on how their PII is used and users have an option whether to provide or not provide this information requested. There will be no penalty or denial of service is attached.
VA SORN #150VA10 Enterprise Identity and Demographics Records-VA2023-24193.pdf (govinfo.gov)

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

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

Individuals have the choice not to provide information.

6.4 <u>PRIVACY IMPACT ASSESSMENT: Notice</u>
Describe the potential risks associated with potentially insufficient notice and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

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

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

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

Privacy Risk: There is a risk that individuals who provide information via Slack will not know how their information is being shared and used internal to the Department of Veterans Affairs.

Mitigation: Use of the Slack service is optional within the VA and individuals may decline to provide information. Safeguards implemented to ensure data is not sent to the wrong VA organization are employee security and privacy training and awareness and required reporting of suspicious activity. Use of secure passwords, access for need-to-know basis, Personal Identification Verification (PIV) Cards, Personal Identification Numbers (PIN), encryption, and access authorization are all measures that are utilized within the facility.

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.***

The procedure for individuals to gain access to their information is as set forth by VA Directive 6213, VA Handbook 6300.3, CFR 38 Part 1&2, CFR 1.460 – 1.474, CFR 1.475 – 1.484, CFR 1.485 – 1.489, CFR 1.490 – 1.4999, CFR 1.500 – 1.527, CFR 1.575 – 1.583, V03208266 Memo SI Notification Process, and FOIA Redaction Memo.
Individuals may submit a request at https://www.foia.gov/ – and select "Create A Request".
VA's Agency FOIA Mailbox is VACOFOIASE@VA.GOV.

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)?

System is not exempt from the access provisions of the Privacy Act.

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

The procedure for individuals to gain access to their information is as set forth by VA Directive 6213, VA Handbook 6300.3, CFR 38 Part 1&2, CFR 1.460 – 1.474, CFR 1.475 –

1.484, CFR 1.485 – 1.489, CFR 1.490 – 1.4999, CFR 1.500 – 1.527, CFR 1.575 – 1.583, V03208266 Memo SI Notification Process, and FOIA Redaction Memo.
Individuals may submit a request at https://www.foia.gov/ – and select "Create A Request".
VA's Agency FOIA Mailbox is VACOFOIASE@VA.GOV.

7.2 What are the procedures for correcting inaccurate or erroneous information?

Describe the procedures and provide contact information for the appropriate person to whom such issues should be addressed? If the correction procedures are the same as those given in question 7.1, state as much. This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

The procedure for individuals to gain access to their information is as set forth by VA Directive 6213, VA Handbook 6300.3, CFR 38 Part 1&2, CFR 1.460 – 1.474, CFR 1.475 – 1.484, CFR 1.485 – 1.489, CFR 1.490 – 1.4999, CFR 1.500 – 1.527, CFR 1.575 – 1.583, V03208266 Memo SI Notification Process, and FOIA Redaction Memo.
Individuals may submit a request at https://www.foia.gov/ – and select "Create A Request".
VA's Agency FOIA Mailbox is VACOFOIASE@VA.GOV.

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

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

The procedure for individuals to gain access to their information is as set forth by VA Directive 6213, VA Handbook 6300.3, CFR 38 Part 1&2, CFR 1.460 – 1.474, CFR 1.475 – 1.484, CFR 1.485 – 1.489, CFR 1.490 – 1.4999, CFR 1.500 – 1.527, CFR 1.575 – 1.583, V03208266 Memo SI Notification Process, and FOIA Redaction Memo.
Individuals may submit a request at https://www.foia.gov/ – and select "Create A Request".
VA's Agency FOIA Mailbox is VACOFOIASE@VA.GOV.

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.

The procedure for individuals to gain access to their information is as set forth by VA Directive 6213, VA Handbook 6300.3, CFR 38 Part 1&2, CFR 1.460 – 1.474, CFR 1.475 – 1.484, CFR 1.485 – 1.489, CFR 1.490 – 1.4999, CFR 1.500 – 1.527, CFR 1.575 – 1.583,

V03208266 Memo SI Notification Process, and FOIA Redaction Memo.
Individuals may submit a request at https://www.foia.gov/ – and select "Create A Request".
VA's Agency FOIA Mailbox is VACOFOIASE@VA.GOV.

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: There is a risk that the information provided through Slack is inaccurate and decisions are made with incorrect information.

Mitigation: The risk of incorrect information in an individual's records is mitigated by authenticating information when possible. Any validation performed would merely be the Veteran personally reviewing the information before they provide it. Individuals are allowed to provide updated information for their records by submitting new forms or correspondence and indicating to the VA that the new information supersedes the previous data.

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 are invited to join Slack by other users that want to communicate and collaborate. Approval of users to join Slack is limited to Slack workspace owner and workspace administrators. Slack uses 2-FA authentication mechanism to allow users to access the system. Slack also uses single sign-on for internal VA users with a Personal Identity Verification PIV card.

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?

Users from other federal agencies that are communicating and collaborating with VA users are invited to join VA's Slack by an existing user. Approval of all users are is limited to Slack workspace owner and workspace administrators. The PII shared is name and email address of other Slack users for purposes of communicating and collaborating.

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.

User roles are member or guest. Members can create private and public channels. Guests are not able to create private and public channels. All users are able to communicate and collaborate with other users in VA's Slack workspace. Slack is a communication and collaboration tool, similar to email. No VA user can make amendments or changes to Slack code.

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.

VA contractors will have access to the name and email address of other Slack users for the purpose of communication and collaboration, similar to email. VA contractors have no role in the design or development of Slack. As a result, there is no need for a confidentiality agreement, Business Associate Agreement (VAA) or Non-Disclosure Agreement (NDA).

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.

Standard TMS HIPAA/Privacy training is required of all VA and contractor users.

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

8.4a If Yes, provide:

1. *The Security Plan Status:* Completed; Signed
2. *The System Security Plan Status Date:* 03/06/2023
3. *The Authorization Status:* Authorization to Operation (ATO) granted
4. *The Authorization Date:* 03/06/2023
5. *The Authorization Termination Date:* 03/05/2026
6. *The Risk Review Completion Date:* 03/03/2023
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* Impact: 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)*

Slack is hosted in a Commercial Cloud Service Provider. FedRAMP Cloud Provider – AWS Cloud. Slack is a Software as a Service (SaaS).

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 contractor establish that VA retains ownership right over data including PII.

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.

Slack do not collect any 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.

This principle is included in the contract with Slack.

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).

This system is not using RPA.

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

Signature of Responsible Officials

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

Lynn A Olkowski

Digitally signed by Lynn A Olkowski
Date: 2024.01.10 11:47:44 -06'00'

Privacy Officer, Lynn Olkowski

JAMES MCGEE

Digitally signed by JAMES MCGEE
Date: 2024.01.10 12:20:50 -07'00'

Information Systems Security Officer, Mark McGee

THOMAS ADAMS

Digitally signed by THOMAS ADAMS
Date: 2024.01.11 07:58:01 -06'00'

Information Systems Owner, Thomas Adams

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).

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