Privacy Impact Assessment for the VA IT System called:

SAP Concur-e.

Veterans Affairs Central Office (VACO)

Financial Services Center (FSC)

eMASS ID #2487

Date PIA submitted for review:

8/28/2024

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Mark A. Wilson	Mark.Wilson@va.gov	512-937-4824
Information System Security Officer (ISSO)	Albert Estacio	Albert.Estacio@va.gov	909 583-6309
Information System Owner	Chino Walters	Chino.Walters@va.gov	202 461-0452

Abstract

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

SAP Concur - e is an enterprise application under the authority of the Financial Service Center. It allows VA employees/Travel Arrangers to create, process travel requests and create vouchers. It allows the administrative users create new profiles and grant user permissions, Approvers to approve, disapprove, and authorize travel requests. The ETS is a comprehensive, end-to-end web-based product that enables VA to plan, book, track, approve, and request reimbursement for official travel services.

The E-Gov Travel Program and the E-Gov Travel Service (ETS) is the E-Gov platform required by the Federal Travel Regulation (FTR) for civilian federal Government travel and serves as the foundation for achieving federal goals for government-wide-travel manage.

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?

Sap Concur – E is owned by the vendor under the E-Gov Travel Program.

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

SAP Concur - e is an enterprise application under the authority of the Financial Service Center. It allows VA employees/Travel Arrangers to create, process travel requests and create vouchers. It allows the administrative users create new profiles and grant user permissions, Approvers to approve, disapprove, and authorize travel requests. The E-Gov Travel Service (ETS) is a comprehensive, end-to-end web-based product that enables VA to plan, book, track, approve, and request reimbursement for official travel services.

The E-Gov Travel Program and the E-Gov Travel Service (ETS) is the E-Gov platform required by the Federal Travel Regulation (FTR) for civilian federal Government travel and serves as the foundation for achieving federal goals for government-wide-travel manage.

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?

There is approximately a total of 180,000 plus VA users in the system. The users are all current and former VA employees and invitational travelers who receive temporary duty benefits.

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

The SAP Concur-e contains pertinent information to facilitate the temporary duty travel to create, process travel requests, and reimbursement vouchers. Information such as the employees name, full physical address to include state and zip code, Individual Billed account charge card number, personal credit card number, personal phone number, personal email, gender, race/ethnicity, emergency contact information, and government email address.

.

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

Travel information is shared internally over sFTP by VLTrader and externally over HTTP with Duluth Sabre. Key information is transmitted to plan, book, track, approve, and request reimbursement for official travel services.

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?*

No

3. Legal Authority and SORN

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

Purchase Credit Card Program-VA (131VA047)

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 has an existing SORN documents, and no modifications are needed at this time.

4. System Changes

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

No Changes in the business process will result from this PIA completion.

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

No Changes in the business process will result from this PIA completion.

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: Individual Billed account charge account, Personal Credit Card Number, Government Email address.

PII Mapping of Components (Servers/Database)

SAP Concur-e consists of 0 key components (servers/databases/instances/applications/software/application programming interfaces (API). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by SAP Concur-e and the reasons for the collection of the PII are in the table below.

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

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

Internal Components Table

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

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

1.2a List the individual, entity, or entities providing the specific information identified above. For example, is the information collected directly from the individual as part of an application for a benefit, or is it collected from other sources such as commercial data aggregators?
The individual traveler is the only source of submitting information into the system. N/A

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.
It allows VA employees/Travel Arrangers to create, process travel requests and create vouchers. The administrative will be able to create new profiles and grant user permissions, such as approving, reporting, arranging, etc.

1.2c Does the system create information (for example, a score, analysis, or report), list the system as a source of information?
No

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?

All travel information is entered by traveler manually in the system. Arrangers can make reservations after profile is created.

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?

There is no official VA form to collect individual information. Each station uses a specific method such as Light Electronic Action Framework (LEAF), email, or self-created form.

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

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

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

The traveler will only have the capability to validate information once entered. FSC administrative staff can check when cards will expire and remove from profile.

Station admin staff is responsible to check roles (arranger, report user, auditor, etc).
This is done semi-annually.

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

No

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

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

The traveler has access to view their SPI data identified in item #1.1 above. The FSC asks the traveler to validate the information prior to initiating a travel authority.

Sorn Site (https://www.oprm.va.gov/privacy/systems_of_records.aspx).
Corporate Travel and Charge
Cards—VA' (131VA047).
govinfo.gov/content/pkg/FR-2023-09-15/pdf/2023-20052.pdf

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: Sensitive personal information can be released to unauthorized individuals.

Mitigation:

• SAP Concur-e adheres to information security requirements instituted by the VA Office of Information Technology (OIT).
• SAP Concur-e relies on accurate information provided by the individual to the VA.
• VA employees are required to take Privacy, HIPAA, and information security training annually.
• File access granted only to those with a valid need to know.
• Only internal VA employees can access SAP Concur.

Section 2. Uses of the Information

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

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

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

PII/PHI Data Element	Internal Use	External Use
Name	File Identification purposes	Used as an identifier
Date of Birth	Used as an identifier	Used as an identifier
Mailing Address	Used to contact the individual and entitlement verification	Used to contact the individual and entitlement verification
Personal credit card	Used to reserve hotels	Used to reserve hotels
Phone Number	Used to contact the individual	Used to contact the individual
Personal Email Address	Used to contact the individual	Used to contact the individual
Individual Billed account charge card number	Used for reimbursement deposit account verification.	Used for reimbursement deposit account verification
Government Email address	Used to contact the individual	Used to contact the individual
Gender	Used to identifier	Used as an identifier
Race/ethnicity	Used to identifier	Used as an identifier
Emergency contact Information	Used to contact the individual	Used to contact the individual

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?

SAP Concur-e processes data reports based on requested criteria ranges and these can be exported to Excel or CSV files for further analysis processing.

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.

If the employee's profile data is updated, any existing travel documents will require a manual update. Future documents the system will replace the new data on the document and save permanently in the system for the individual.

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?

All PII is masked in user interface in all environments and encrypted during transmission via Secure Sockets Layer (SSL). The address and telephone number is viewable only to Arranger & Admin at rest and all other PII is masked.

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

We don't store SSN in SAP Concur-e.

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

All PII is masked in user interface in all environments and encrypted during transmission via Secure Sockets Layer (SSL). The address and telephone number is viewable only to Arranger & Admin at rest and all other PII is masked. PII is masked in database and viewable to authorize personal only.

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information.

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

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

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

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

2.4a How is access to the PII determined?

Access is approved by employee supervisors and granted by local administrator.

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

VA employees are required to take Privacy, HIPAA, and information security training annually.

2.4c Does access require manager approval?

Yes, based on role.

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

Access to PII is tracked and masked for security The traveler address and telephone number is viewable only to Traveler, Arranger, & Admin.

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

All personal and application based on request.

Section 3. Retention of Information

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

3.1 What information is retained?

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

- Name
- Address
- Date of Birth
- IBA charge card
- vendor code
- Phone number.
- Email
- Gender
- Race/ethnicity.
- Emergency contact

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.*

Records are retained if required per National Archivist and Records Administration (NARA) standards (Reference: GRS Schedule 1.1, Item #10). Destroy 6 years after final payment or cancellation, but longer retention is authorized if required for business use.

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

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

https://www.archives.gov/files/records-mgmt/grs/grs01-1.pdf NARA GRS 1.1 item #10 (Disposition Authority DAA-GRS-2013-0003-0001) identifies records documenting the movement of goods and persons under government orders to be maintained for the specified retention period.

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.

In accordance with VA6500.1; the electronic records are retained if required (GRS Schedule 1.1, Item #10), and are destroyed in accordance with National Archives and Records Administration disposition instructions. [Destroy 6 years after final payment or cancellation, but longer retention is authorized if required for business use.] We are also finalizing procedures to automate the destruction of media at the appropriate time based on published NARA and VA instructions (nightly job that removes data outside of retention period deletes / destroys metadata and image to re-use file storage).

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.

SAP Concur-e uses testing sites for training and testing purposes. These testing sites do not have actual PII data and fictitious information is used as a filler in these locations. PII information is not used for searching data within the system, instead the employee's name or Travel Authority number is used for all research.

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: If information is retained longer than specified, privacy information is protected for not releasing to unauthorized individuals.

Mitigation: SAP Concur-e follows GRS Schedule1.1, Item #10. All information is stored for 6 years—due to business need—and is then destroyed following the procedures listed in 3.4.

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***
VL Trader	Process documents to accounting system	• Name • Address • Date of Birth • Individual Billed account charge card number • Personal credit card number • Personal Phone number • Personal Email • Government Email address • Gender • Race/ethnicity • Emergency contact Information	SFTP

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: Privacy information can be released to unauthorized individuals.

Mitigation: SAP Concur adheres to information security requirements instituted by the VA Office of Information Technology (OIT).
• VA employees are required to take Privacy, HIPAA, and information security training annually.
• Information is shared in accordance with VA Handbook 6500
• File access granted only to those with a valid need to know
• Controls in place are station review of access requests followed by FSC review of access requests. All access requests are logged and recorded by who requested access and those approving access.

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***
Duluth Sabre	Book travel arrangements	• Name • Address • Date of Birth • Individual Billed account charge card number	MOU with GSA	HTTPS

		• Personal credit card number • Personal Phone number • Personal Email • Government Email address • Gender • Race/ethnicity • Emergency contact Information		

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: Privacy information can be released to unauthorized individuals.

Mitigation: SAP Concur-e adheres to information security requirements instituted by the VA Office of Information Technology (OIT).
• VA employees are required to take Privacy, HIPAA, and information security training annually.
• Information is shared in accordance with VA Handbook 6500
• File access granted only to those with a valid need to know
• Controls in place are station review of access requests followed by FSC review of access requests. All access requests are logged and recorded by who requested access and those approving access.

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.

SAP Concur-e collects PII/PHI information directly from VA employees. System of Records Notice SORN is clear about the use of the information, specifically SORN: 13VA047 Individuals Submitting Invoices-Vouchers for Payment-VAhttps://www.govinfo.gov/content/pkg/FR-2020-04-23/pdf/2020-08611.pdf.

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

Privacy Act notice must be agreed upon before continuing logging into the system.

WARNING

This is a U.S. Federal Government information system that is "FOR OFFICIAL USE ONLY." Unauthorized access is a violation of U.S. Law and may result in criminal or administrative penalties. Users shall not access other users' or system files without proper authority. Absence of access controls is NOT authorization for access! Information systems and equipment related to E-Gov Travel Service are intended for communication, transmission, processing, and storage of U.S. Government information. These systems and equipment are subject to monitoring by law enforcement and authorized officials Monitoring may result in the acquisition, recording, and analysis of all data being communicated, transmitted, processed, or stored in this system by law enforcement and authorized officials. Use of this system constitutes consent to such monitoring.

PRIVACY ACT NOTICE

This system contains information protected under the provisions of the Privacy Act of 1974 (Public Law 93-579). Less

Any privacy information displayed on the screen or printed must be protected from unauthorized disclosure. Employees who violate privacy safeguards may be subject to disciplinary actions, a fine of up to $5,000, or both.

"The information requested in the ConcurGov is collected pursuant to Executive Order 9397 and Chapter 57, Title 5 United States Code. The purpose of the collection is to establish a comprehensive travel services system which enables travel service providers to authorize, issue, and account for travel and travel reimbursements provided to individuals on official Federal Government business. Categories of records in the system records may include: Full name matching the form of ID used for travel; Social Security Number; employee identification number; home, office, agency and emergency contact information; travel and hotel preferences; current passport and/or visa number(s); credit card numbers and related information; bank account information; frequent traveler account information (e.g., frequent flyer account numbers); date of birth; gender; DHS redress and known traveler numbers (numbers DHS assigns to promote resolution with previous watch list alerts and facilitate passenger clearance, respectively); trip information (e.g., destinations, reservation information); travel authorization information; travel claim information; monthly reports from travel agent(s) showing charges to individuals, balances, and other types of account analyses; and other official travel related information.

Routine uses which may be made of the collected information and other financial account information in the system(s) of record entitled "Contracted Travel Services Program GSA/GOVT-4" are: (a) To another Federal agency, Travel Management Center (TMC), online booking engine suppliers and the airlines that are required to support the DHS/TSA Secure Flight program. (b) To a Federal, State, local, or foreign agency responsible for investigating, prosecuting, enforcing, or carrying out a statute, rule, regulation, or order, where agencies become aware of a violation or potential violation of civil or criminal law or regulation; (c) To another Federal agency or a court when the Federal Government is party to a judicial proceeding; (d) To a Member of Congress or a congressional staff member in response to an inquiry from that congressional office made at the request of the individual who is the subject of the record; (e) To a Federal agency employee, expert, consultant, or contractor in performing a Federal duty for purposes of authorizing, arranging, and/or claiming reimbursement for official travel, including, but not limited to, traveler profile information; (f) To a credit card company for billing purposes, including collection of past due amounts; (g) To an expert, consultant, or contractor in the performance of a Federal duty to which the information is relevant; (h) To a Federal agency by the contractor in the form of itemized statements or invoices, and reports of all transactions, including refunds and adjustments to enable audits of charges to the Federal Government; (i) To a Federal agency in connection with the hiring or retention of an employee; the issuance of security clearance; the reporting of an investigation; the letting of a contract; or the issuance of a grant, license, or other benefit to the extent that the information is relevant and necessary to a decision; (j) To an authorized appeal or grievance examiner, formal complaints examiner, equal employment opportunity investigator, arbitrator, or other duly authorized official engaged in investigation or settlement of a grievance, complaint, or appeal filed by an employee to whom the information pertains; (k) To the Office of Personnel Management (OPM), the Office of Management and Budget (OMB), or the Government Accountability Office (GAO) when the information is required for program evaluation purposes; (l) To officials of labor organizations recognized under 5 U.S.C. Chapter 71 when relevant and necessary to their duties of exclusive representation concerning personnel policies, practices, and matters affecting working conditions; (m) To a travel services provider for billing and refund purposes; (n) To a carrier or

an insurer for settlement of an employee claim for loss of or damage to personal property incident to service under 31 U.S.C. § 3721, or to a party involved in a tort claim against the Federal Government resulting from an accident involving a traveler; (o) To a credit reporting agency or credit bureau, as allowed and authorized by law, for the purpose of adding to a credit history file when it has been determined that an individual's account with a creditor with input to the system is delinquent; (p) summary or statistical data from the system with no reference to an identifiable individual may be released publicly; (q) to the National Archives and Records Administration (NARA) for records management purposes; (r) to appropriate agencies, entities, and persons when (1) The Agency suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (2) the Agency has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by GSA or another agency or entity) that rely upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with GSA's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm. Information requested is voluntary, however, failure to provide the information may nullify the ability to book online travel reservations."

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.

Privacy Act notice must be agreed upon before continuing logging into the system.

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.

Mandatory; VA employees will not be paid travel benefits unless their information is obtained and used to process the payment.

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.
SAP Concur-e collects PII/PHI information directly from VA employees. Nevertheless, if an individual wish to remove consent for a particular use of their information, they should contact their servicing administrator or remove it.

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: Privacy information can be collected prior to providing the written notice to individuals.

Mitigation:
• Privacy Act notice must be agreed upon before continuing logging into the system
• All information is collected directly from individual VA employees only.
• Information is used to process travel and payments.

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.***

SAP Concur-e collects PII/PHI information directly from VA Employees. VA employees may access their information by contacting their servicing administrator.

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)?

No exemption

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?

Privacy Act notice must be agreed upon before continuing logging into the system

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.

SAP Concur-e collects PII/PHI information directly from VA Employees. VA employees may access their information by contacting their servicing administrator.

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.

Typically, it is the employee who brings this information to our attention. They are then notified manually at that time. Typically, either via telephone or e-mail.

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.

SAP Concur-e collects PII/PHI information directly from individuals. Nevertheless, VA employees can contact their servicing administrator.

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: Inaccurate data may not be used to process payments.

Mitigation: Once it has been determined a payment has been sent to the wrong account. The employee is contacted, required to submit a new 10091 banking form Via self-service portal. Once the submission is received, it is sent to the Vendorizing Team to update the banking information in FMS & iFAMS, and the payment is resubmitted.

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?
Individuals must take and pass training on Privacy, HIPAA, information security, and government ethics.
• Once training is complete, a request is submitted for access. Before access is granted; this request must be approved by the supervisor, Information System Security Officer (ISSO), and OIT.

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?
No other agencies have access the system.

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.

Federal Traveler = Traveler in SAP Concur-e
Authorized Support Contacts = ability to enter support cases in SAP Concur-e
Federal Approver = assigned approvers to approve travel or vouchers
Federal Auditor (Read only) = read only access to system for auditing
Federal Travel Arranger = ability to arrange travel or prepare vouchers for travelers
Global Admin = FSC only TSQA Team. Highest admin level to maintain system preferences. Ability to route certain documents for 2nd level approval and ability to view both Admin and Routing List Admin.
Local Admin = Travel coordinator for travelers SAP Concur-e system needs
Report User = Intelligence Reports from Cognos with travel related data
Routing List Admin = the ability to create and update routing list (routes the travelers document for approval)
System Admin = FSC ONLY Travel Operations Team to completed Local Admin functions
TMC Support = Unknown. Not used at this time

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.
• Contractors will have access to the system and their contracts are reviewed on an annual basis.
• Contractors must take and pass training on Privacy, HIPAA, information security, and government ethics.
• Contractors must have a completed security investigation.
• Once training and the security investigation are complete, a request is submitted for access, before access is granted, this request must be approved by the government supervisor, Information System Security Officer (ISSO), and Office of Information & Technology (OIT).

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.

Privacy and Information Security Awareness and Rules of Behavior (TMS course # 10176) is required for all Federal and Contractor personnel that require access to the VA Network. Annual training compliance is closely monitored. Other required Talent Management System courses monitored for compliance: VA 10203: Privacy and HIPAA Training VA 3812493: Annual Government Ethics

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

8.4a If Yes, provide:

1. *The Security Plan: Approved.*
2. *The System Security Plan Status Date: 7*/15/2024
3. *The Authorization Status:* Authorized through 3/22/2024.
4. *The Authorization Date:* 3/22/2024
5. *The Authorization Termination Date:* 3/22/2025
6. *The Risk Review Completion Date:* 3/8/2024
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* Moderate

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

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

Section 9 – Technology Usage

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

9.1 Does the system use cloud technology? If so, what cloud model is being utilized?

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

Note: For systems utilizing the VA Enterprise Cloud (VAEC), no further responses are required after 9.1*. (Refer to question 3.3.1 of the PTA)*

Yes. Azure Gov Cloud

9.2 Does the contract with the Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII? (Provide contract number and supporting information about PII/PHI from the contract). (*Refer to question 3.3.2 of the PTA) This question is related to privacy control AR-3, Privacy Requirements for Contractors, and Service Providers.*

Yes

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, and VA will maintain ownership.

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.

SAP Concur-e is a System as a Service (SaaS) used by FSC.

The AWS GovCloud is under contract as Cloud Provider in VAEC. The Cloud Provider is only accountable for the security controls and privacy of data it has been explicitly approved to manage. All other security controls are implemented locally by the FSC organization or shared amongst enterprise VA systems.

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).

Sap Concur -e-will not have an RPA component.

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

MARK WILSON

Digitally signed by MARK WILSON
Date: 2024.09.20 10:39:33 -05'00'

Privacy Officer, Mark A. Wilson

ALBERTINO ESTACIO

Digitally signed by ALBERTINO ESTACIO
Date: 2024.09.26 10:32:35 -07'00'

Information System Security Officer, Albert Estacio

CHINO WALTERS

Digitally signed by CHINO WALTERS
Date: 2024.09.20 10:27:15 -04'00'

Information System Owner, Chino Walters

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).

SORN: 13VA047 Individuals Submitting Invoices-Vouchers for Payment-VAhttps://www.govinfo.gov/content/pkg/FR-2020-04-23/pdf/2020-08611.pdf.

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