Privacy Impact Assessment for the VA IT System called:

Foreign Travel Portal (FTP)

Veterans Affairs Central Office (VACO)

Corporate Travel & Charge Card Services (CTCCS)

eMASS ID # 2274

Date PIA submitted for review:

May 23, 2024

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Pamela M. Smith	Pamela.Smith6@va.gov	512-937-4824
Information System Security Officer (ISSO)	Ronald Murray	Ronald.Murray2@va.gov	512-460-5081
Information System Owner	Jonathan M. Lindow	Jonathan.Lindow@va.gov	512-568-0626

Abstract

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

The Foreign Travel Portal is an electronic system in which travelers and travel arrangers submit all foreign travel packages for review and approval. The portal is a repository that captures all required documentation that would assist with timely approval routing as outlined a VA travel policy. The FTP provide end to end automation and foreign travel approval management for the travel logistics section and improves the accuracy of foreign travel reporting with VA-wide usage. Ultimately, the portal improves oversight and accountability of all foreign travel requests while also automating the reporting mechanisms which allows the VA to provide accurate quarterly reports for ALL VA Foreign travel. This system contains a free text comment section.

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?*

Foreign Travel Portal (FTP) and Corporate Travel and Charge Card Service (CTCCS) owns the system.

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

Foreign Travel Portal (FTP): Corporate Travel and Charge Card Service (CTCCS) includes the Foreign Travel program, and the Finance Services Center (FSC) houses the Web Foreign Travel program (FileNet (Store Data and Mask PII). The Foreign Travel Portal is a minor under Permanent Change of Station (PCS) System. The purpose of this system is to serve as a repository that captures all required documentation that would assist with timely approval routing as outlined a VA travel policy. The FTP provide end to end automation and foreign travel approval management for the travel logistics section and improves the accuracy of foreign travel reporting with VA-wide usage. Ultimately, the portal improves oversight and accountability of all foreign travel requests while also automating the reporting mechanisms which allows the VA to provide accurate quarterly reports for ALL VA Foreign travel. The FTP contains pertinent information to facilitate issuance of government passport and visa such as the employees name, full physical address to include state and zip code, last four of social security number, phone number, email address, date of birth, phone number (personal/VA), email (personal/VA), Emergency contact information, Passport #/Expiration date (personal/government issued) and eligible family members and declared dependents. The system stores PI information of employees as further explained in section 1.1. FTP system adheres to information security requirements instituted by the VA Office of Information Technology (OIT) to protect the sensitive data. The contracted companies used by VA all have a Memorandum of Understanding (MOU) or contract signed through the VA Contracting Office. The companies do not

access this VA system. The system will be sharing information internally, as discussed in section 4, and externally, as discussed in question 5. The legal authority we follow is the General Records Schedule (GRS) 2.2; Employee Management Records/ Item 090 – Records related to official passports. The completion of the PIA will not result in any business or technology changes. The system does not use cloud technology. There is a total of approx. 625 VA users in the system. The users are all current or former VA employees that requested approval for foreign travel. Profiles are created for requesting traveler when the VA form 0900 are initiated by the requesting employee. User profiles are never deleted from the system; however, access will be revoked if the user does not login for 90 days. This is a standalone system located at the FSC. The sharing of information is covered in SORN 131VA047, Purchase Credit Card Program-VA.

C. *Who is the owner or control of the IT system or project?*
Financial Technology Service Va owned and VA 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?*

150,000 VA employees & Veterans or Dependents

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

The Foreign Travel Portal is an electronic system in which travelers and travel arrangers submit all foreign travel packages for review and approval. The portal is a repository that captures all required documentation that would assist with timely approval routing as outlined a VA travel policy. The FTP provide end to end automation and foreign travel approval management for the travel logistics section and improves the accuracy of foreign travel reporting with VA-wide usage. Ultimately, the portal improves oversight and accountability of all foreign travel requests while also automating the reporting mechanisms which allows the VA to provide accurate quarterly reports for ALL VA Foreign travel. This system contains a free text comment section. The text box is being monitored and a privacy statement not to include PII/PHI has been added.

Below is additional description of information.
Name
Last four of Social Security Number
Date of Birth
Mailing address
Zip Code
Phone Number (personal/VA)
E-Mail Address (personal/VA)
Passport # Expiration Date
(personal/government issued

The purpose is to process and track overseas travel request and arrangements.

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

The system shares key PII information listed in 2E with Department of State Special Issuance Agency Applicable Embassies. A manual validation process is used to capture required Personal Information for transmission to Department of Station. There are no modules or subsystems used to capture this data.

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 usedacross sites?*

Yes. The System is only at Financial Service Center

3. Legal Authority and SORN

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

48 CFR 13; 31 U.S.C. 3511; VA Financial Policy, vol. XIV; Federal Acquisition Regulation (FAR) part 13; 48 CFR part 13; and Public Law 93–579 section 7(b)

Purchase Credit Card Program-VA (131VA047)
govinfo.gov/content/pkg/FR-2023-09-15/pdf/2023-20052.pdf

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

No

4. System Changes

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

No

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

No

Section 1. Characterization of the Information

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

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

Identify and list all Sensitive Personal Information (SPI) that is collected and stored in the system, including Individually Identifiable Information (III), Individually Identifiable Health Information (IIHI), Protected Health Information (PHI), and Privacy- Protected Information. For additional information on these information types and definitions, please see VA Directives and Handbooks in the 6500 series

(https://vaww.va.gov/vapubs/). If the system creates information (for example, a score, analysis, or report), list the information the system is responsible for creating.

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

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

Additional Data elements
• Passport # Expiration Date (personal/government issued)
- Use to notify State Department for emergency situations

PII Mapping of Components (Servers/Database)

FTP consists of 1 key component. The one component has been analyzed to determine if any PII is collected. The type of PII collected by FTP and the reasons for the collection of PII are in the table below.

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

Internal Components Table

Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
FileNet	Yes	Yes	• Name • Last four of Social Security Number • Date of Birth • Mailing address • Zip Code • Phone Number (personal/VA) • E-Mail Address (personal/VA) • Passport # Expiration Date (personal/government issued	Overseas travel reporting	Encrypted at rest and in transit.

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

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

The information provided above is provided by the Individual/travel coordinator when requesting official travel overseas.

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.

Traveler coordinators from Office of Inspector General (OIG), Veterans Health Administration (VHA), Veterans Business Administration (VBA), National Cemetery Administration (NCA), and other VA Staff Offices manually input the information into the Foreign Travel Portal (FTP) System by the approved representative. The relocating employee then verifies the information as correct.

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

The traveling employee/travel arranger uploads VA form 0900 to the foreign travel portal for visibility to Finance Services Center (FSC)/ Corporate Travel and Charge Card Service (CTCCS)/Travel Logistics Conference Division (TLCD). The collected data allows FSC/CTCCS/TLCD to confirm the identity and validity of the requesting traveler and draft required letters or authorization for issuance of government passport, visa and country clearance.

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?

The information provided above is provided by the requesting traveler and/or traveler arranger at the traveling employees station/office including but not limited to VHA, NCA, VBA, BVA and other VA staff offices. The information is required on VA Form 0900 to initiate a profile in the foreign travel portal ultimately allowing the travel logistic team to coordinate with Department of State and applicable embassies for government passport, visa and country clearance. Shortly after submitting VA Form 0900 in the portal, instructions are sent via outlook to traveler based on the input of the above information on VA Form 0900.

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?

VA Form 0900 and no OMB control number

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 purpose of the information is to ensure the correct individuals are receiving foreign travel entitlements. Also, that the authorized travel entitlements are in accordance with the Federal travel Regulations and VA travel Policy mitigating potential underpayments and over payments. Information is verified manually for every travel episode by a processing agent visual inspection of requested submissions.

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. Information is verified manually for every travel episode by a processing agent visual inspection of requested submissions.

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

Federal Passport Agent's Reference Guidance (Fed PARG)

The purpose of the information is to ensure the correct individual is receiving the government passport, visa, and country clearance prior to traveling in an official capacity. Department of State requires passport agents at the VA to validate the validly of the application details before routing packages for processing. Also, employees traveling in an official capacity must travel with a government passport in accordance with the Federal Travel Regulations. The traveling employee and/or travel arranger has access to view their sensitive personal information (SPI) data identified in item #1.1 above. The FSC travel logistics team reviews the data to validate the information prior to coordinating with Department of State and applicable embassies.

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 may be released to unauthorized individuals.

Mitigation:
•FTP adheres to information security requirements instituted by the VA Office of Information Technology (OIT).
•FTP relies on information previously collected by the VA from the individuals.
•Both VA contractors and VA employees are required to take Privacy, Health Insurance Portability and Accountability Act (HIPAA), and information security training annually.
•File access granted only to those with a valid need to know and access privileges

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	Used to identify the traveler & communicate	same as Internal use
Social Security Number	last four as patient identifier/verification	same as Internal use
Date of Birth	identify age and confirm travelers' identity	same as Internal use
Mailing Address	mail issued passport to traveler	same as Internal use
Phone Number	contact the traveler	same as Internal use
Email Address	contact the traveler	same as Internal use
Passport Number/ Issue date/Expiration date	facilitate country clearance	same as Internal use
Emergency Contact	required for country clearance request	same as Internal use

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

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

The business users perform a manual process to review data because the application doesn't have an automatic analytical process or tools.

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 or request is updated, the system replaces the data on the document that is populated on the foreign travel portal travelers' grid and reporting.

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 will be masked in user interface in all environments and encrypted during transmission via FileNet. Visibility restrictions showing PII information masked with XXXXX. Viewable to traveler, Foreign Travel Portal Admins, and FSC Help desk. Editable only by Foreign Travel Administrators.

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

Visibility restrictions showing PII information masked with XXXXX. Viewable to traveler, FTP Staff, Editable only by FTP Admin POCs

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

All PII will be masked in user interface in all environments and encrypted during transmission via FileNet. Visibility restrictions showing PII information masked with XXXXX. Viewable to traveler, Foreign Travel Portal Admins, and FSC Help desk. Editable only by Foreign Travel Administrators.

2.4 <u>PRIVACY IMPACT ASSESSMENT: Use of the information.</u>

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 determined based on he/she role and individual must complete appropriate training.

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

- System access is granted based on an access request in VA's Online Form Submission System (OFS). Access is approved by FSC managers and station approving officials with approving authority.
- The foreign travel portal adheres to information security requirements instituted by the VA Office of Information Technology (OIT)
- The foreign travel portal relies on information previously collected by VA form 0900 from the traveler and/or traveler arranger.
- VA employees are required to take Privacy, HIPAA, and information security training annually.
- Only VA employees can access the foreign travel portal.
- System of Records Notice (SORN) is clear about the sharing of information, specifically Purchase Credit Card Program- VA (131VA047)

2.4c Does access require manager approval?

Yes

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

Monitored and tracked.

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

Data administrator and security Section 3. Retention of Information

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

Section 3. Retention of Information

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

3.1 What information is retained?

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

The information listed in 1.1 that we collect.

- Name
- Last four of Social Security Number
- Date of Birth
- Personal Mailing Address
- Phone (personal/VA)
- Email (personal/VA)
- Emergency Contact Information (Name, Phone, Email)
- Passport Number, Expiration Date (personal and government)

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 General Records Schedule (GRS) 2.2 Item 090; Records related to official passports standards. Destroy when 3 years old or upon employee separation or transfer, whichever is sooner; 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, GRS Schedule 1.1, Item #10, Disposition Authority DAA-GRS-2013-0003-0001 https://www.archives.gov/files/records-mgmt/grs/grs01-1.pdf

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

GRS Schedule 1.1, Item #10, Disposition Authority DAA-GRS-2013-0003-0001 https://www.archives.gov/files/records-mgmt/grs/grs01-1.pdf

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

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

In accordance with VA 6500.1; the electronic records are retained if required (GRS Schedule 2.2, Item #090), and are destroyed in accordance with National Archives and Records Administration disposition instructions. Destroy when 3 years old or upon employee separation or transfer, whichever is sooner; but longer retention is authorized if required for business use.

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.

The Foreign Travel Portal System 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 Date's 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 may be released to unauthorized individuals.
Mitigation: All information in the foreign travel portal is stored for 3 years and then destroyed following 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***
N/A	N/A	N/A	N/A

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

Discuss the privacy risks associated with the sharing of information within the Department and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

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

Follow the format below:

Privacy Risk:
Privacy information may be released to unauthorized individuals.

Mitigation:

- • System access is granted based on an access request in VA's Online Form Submission System (OFS). All access requests are logged and recorded by who requested access and those approving access.
- Access is approved by FSC managers and station approving officials with approving authority.
- The foreign travel portal adheres to information security requirements instituted by the VA Office of Information Technology (OIT)
- The foreign travel portal relies on information previously collected by VA form 0900 from the traveler and/or traveler arranger.
- Information is shared in accordance with VA Handbook 6500
- File access granted only to those with a valid need to know.
- Only VA employees can access the foreign travel portal.
- System of Records Notice (SORN) is clear about the sharing of information, specifically Purchase Credit Card Program-VA (131VA047)
- System access is granted based on an access request in VA's Online Form Submission System (OFS). All access requests are logged and recorded by who requested access and those approving access.
- Access is approved by FSC managers and station approving officials with approving authority.
- The foreign travel portal adheres to information security requirements instituted by the VA Office of Information Technology (OIT)
- The foreign travel portal relies on information previously collected by VA form 0900 from the traveler and/or traveler arranger.
- Information is shared in accordance with VA Handbook 6500
- File access granted only to those with a valid need to know.

- Only VA employees can access the foreign travel portal.
- System of Records Notice (SORN) is clear about the sharing of information, specifically Purchase Credit Card Program-VA (131VA047)

Section 5. External Sharing/Receiving and Disclosure

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

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

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

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

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

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

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

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

Data Shared with External Organizations

List External Program Office or IT System information is shared/received with	***List the purpose of information being shared / received / transmitted with the specified program***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted)with the Program or IT system***	***List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)***	***List the method of transmission and the measures in place to secure data***

	office or IT system			
Department of State Special Issuance Agency Applicable Embassies	Allow individual traveler authority to make overseas travel arrangements	• Name • Last four of Social Security Number • Date of Birth • Mailing address • Zip Code • Phone Number (personal/VA • E-Mail Address (personal/VA) • Passport # Expiration Date (personal	Department of State IAA Number: 1931J818Y7024 CTCCS Courier Support Service: Contract/BPA: 36C10X21A00111	Encrypted email via Outlook Courier Delivery Service

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 may be released to unauthorized individuals.

Mitigation:
- System access is granted based on an access request in VA's Online Form Submission System (OFS). All access requests are logged and recorded by who requested access and those approving access.
- Access is approved by FSC managers and station approving officials with approving authority.
- The foreign travel portal adheres to information security requirements instituted by the VA Office of Information Technology (OIT)
- The foreign travel portal relies on information previously collected by VA form 0900 from the traveler and/or traveler arranger.
- Information is shared in accordance with VA Handbook 6500
- File access granted only to those with a valid need to know.
- Only VA employees can access the foreign travel portal.

- System of Records Notice (SORN) is clear about the sharing of information, specifically Corporate Travel and Charge Cards -VA (131VA047)

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.

Yes, see sample below:
Thank you much for your inquiry on the foreign travel process. In an effort to begin the foreign travel process, one must first access the Foreign Travel Portal and follow the steps. The traveler will be prompted to complete the VA Form 0900 Country Clearance, save and then upload in the Foreign Travel Portal. Once submitted our office will review the travelers VA Form 0900 and provide applicable instructions to obtain a government passport and/or visa based on your foreign travel request. Should you need assistance preparing and submitting your foreign travel request, please see the attached Job Aid.

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

SORN is provided to the public.

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

6.1c Describe how the notice provided for the collection of information is adequate to inform those affected by the system that their information has been collected and is being used appropriately. Provide information on any notice provided on forms or on Web sites associated with the collection.

The business users are not confirming the collected information to ensure it's being used appropriately.
The provided SORN explains the reason, purpose, authority, and routine uses of the collected information is adequate to inform those affected by the system that their information has been collected and is being used appropriately.

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
.

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; Yes, they have the right decline to provide. However, passport, visa and country clearance issuance cannot take place without the required PI details.VA employees will not be approved for foreign travel without the required details.

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.

Currently consent for specific use of his or her information is not offered as the data is only used to facilitate passport, visa and country clearance processing and issuance. Passport, visa and country clearance issuance cannot take place without the required.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

Describe the potential risks associated with potentially insufficient notice and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

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

Principle of Transparency: Has sufficient notice been provided to the individual?

Principle of Use Limitation: Is the information used only for the purpose for which notice was provided either directly to the individual or through a public notice? What procedures are in place to ensure that information is used only for the purpose articulated in the notice?

This question is related to privacy control TR-1, Privacy Notice, AR-2, Privacy Impact and Risk Assessment, and UL-1, Internal Use.
Follow the format below:

Privacy Risk:
Potential insufficient notice of private information being released to unauthorized individuals.

Mitigation:
- System access is granted based on an access request in VA's Online Form Submission System (OFS). All access requests are logged and recorded by who requested access and those approving access.
- Access is approved by FSC managers and station approving officials with approving authority.
- The foreign travel portal adheres to information security requirements instituted by the VA Office of Information Technology (OIT)
- The foreign travel portal relies on information previously collected by VA form 0900 from the traveler and/or traveler arranger.
- Information is shared in accordance with VA Handbook 6500
- File access granted only to those with a valid need to know.
- Only VA employees can access the foreign travel portal.
- System of Records Notice (SORN) is clear about the sharing of information, specifically Purchase Credit Card Program-VA (131VA047)

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 employee will email InternationalTravelServices@va.gov to gain access to their information.

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

The system is Non-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?

Non-exempt from Privacy Act System responsibilities.

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.

Active FTP users can access their profiles and/or travel episodes to correct information. In active FTP user will send an email to InternationalTravelServies@va.gov to gain access which will allow the updates.

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.

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.

7.5 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 be used during foreign travel processing.

Mitigation:
Active FTP users can access their profiles and/or travel episodes to correct information. In active FTP user will send an email to InternationalTravelServies@va.gov to gain access which will allow the updates.

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?

System access is granted based on an access request in VA's Online Form Submission System (OFS). Access is approved by FSC managers and station-approving officials with approving authority. The foreign travel portal adheres to information security requirements instituted by the VA Office of Information Technology (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?

Only VA employees can be granted access to the FTP.

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 – traveler/traveler arranger
- Admin POC – team providing oversight to ensure appropriate travel entitlements. Team also responsible for coordinating with the Department of State and Applicable embassy's regarding issuance of government passport, visa, country clearance etc.
- POC Manager – provides oversight to admin POCs including travel request assignments, register users' visibility and FTP reporting, limited system admin access functionality.
- Superuser role – Program manager – with full functionality including system access.

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.

VA employees are required to take Privacy, HIPAA, and information security training annually. 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 Status:* Approved
2. *The System Security Plan Status Date:* January 6, 2021
3. *The Authorization Status: Authority to Operate*
4. *The Authorization Date:* Granted December 14, 2022
5. *The Authorization Termination Date: September 21, 2026*
6. *The Risk Review Completion Date:* September 10, 2018
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* High

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)*

No, this section is not applicable as it does not use cloud technology.

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.*

No, this section is not applicable as it does not use cloud technology.

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.

No, this section is not applicable as it does not use cloud technology.

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).

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

PAMELA SMITH

Digitally signed by PAMELA SMITH
Date: 2024.06.24 16:39:05 -05'00'

Privacy Officer, Pamela M. Smith

RONALD MURRAY

Digitally signed by RONALD MURRAY
Date: 2024.06.25 06:06:30 -05'00'

Information Systems Security Officer, Ronald Murray

JONATHAN LINDOW

Digitally signed by JONATHAN LINDOW
Date: 2024.06.25 08:40:17 -05'00'

Information Systems Owner, Jonathan M. Lindow

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