Privacy Impact Assessment for the VA IT System called:

VA Time and Attendance System - Cloud (VATAS)

Financial Payroll Services

VA Central Office

Date PIA submitted for review:

08/08/2023

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	*Mark A. Wilson*	*Mark.Wilson@va.gov*	*(512) 386-2246*
Information System Security Officer (ISSO)	*Rito-Anthony Brisbane*	*Rito-Anthony.Brisbane@va.gov*	*(512) 460-5081*
Information System Owner	*Jonathan Lindow*	*Jonathan.Lindow@va.gov*	*(512) 460-5307*

Abstract

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

VA Time and Attendance System - Cloud (VATAS) is a Commercial-Off-The-Shelf (COTS) customizable, web-based Time and Attendance System (TAS) that replaced the Enterprise Time and Attendance (ETA) system. VATAS will be used by all VA employees to request leave, and review leave balance data. VATAS transmits time and leave data to Defense Finance Accounting Services' Payroll Syst. VATAS provides payroll processing services.

Overview

The overview is the most important section of the PIA. A thorough and clear overview gives the reader the appropriate context to understand the responses in the PIA. The overview should contain the following elements:

1 General Description

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

VA Time and Attendance System - Cloud (VATAS); Program Office: Financial Payroll Service (FPS)

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

Conduct Work Schedule and Leave Management designs, develops, and implements leave and work schedule policies and programs that attract, retain, and meet the work-life needs of employees in accordance with law and regulations. Develops and implements policies to administer leave and work schedules in support of agency missions and goals. Coordinates with organizations to provide for the appropriate conveyance of policies, programs, human resources, payroll, and time and attendance systems supporting accurate and timely benefits for employees.

The Financial Services Center (FSC) is the Business Owner of the VATAS application, and it is managed on their behalf by Cognosante.

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

VA owned, Ownership of VATAS Cloud systems fall under the Financial Service Center (FSC); Cognosante personnel work to keep the VATAS Solution up to date with all latest software security patches and new software applications as appropriate.

2. Information Collection and Sharing

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

The number of employees estimated to be in the system at full deployment is approximately 400,000 users.

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

VATAS is an enterprise-wide system which tracks time and attendance for the entire VA. Every two weeks the system uses the information gathered on timesheets to run payroll. Veterans Information Systems (IS) are vital to the Department of Veterans Affairs (VA) business processes; therefore, it is critical that services provided by Veterans Affairs Time and Attendance System, (VATAS) operate effectively without excessive or prolonged interruption The VATAS is hosted by VAEC AWS GovCloud. The Department of Veterans Affairs (VA) Office of Financial Business Operations (OFBO) provides financial systems and operations services to VA administrations and staff offices. Among its responsibilities is enterprise-wide time reporting in support of accounting and personnel benefit services. The time and attendance that supports these functions for OFBO is the Veterans Affairs Time and Attendance System (VATAS). Specifically, VATAS performs these functions: 1) Create new employee profile; update and edit current employee information. 2) Configure various employee groupings, including duty stations and time and leave (T&L) groups. 3) Configure tours of duty Process employee leave requests, overtime/comp time requests, environmental differential requests and related requests. 4) Process/adjust timecards/prior pay period(s). 5) Process timecards for the current pay periods Adjust timecards from prior pay periods. 6) Validate entered timecard information against VA business rules, both at the time of data entry and when issuing batch feeds to external systems. 7) Provide exception reports to identify data anomalies. 8) Provide standard reports to support management and analysis related to T&A. 9) Reconcile timecard information with DCPS. 10) Reconcile employee configuration with HR information in HRSMART. 11) Manage and configure holidays, tours of duty, duty stations, HRSMART database lookup codes, and Time and Leave (T&L) Group

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

VATAS accepts employee profile data from HRSMART, sends time and leave information to DCPS via Systems Automation Data (SDA) interface, receives leave balances from DCPS, and stores data on the VATAS database.

The core VATAS application is a web-based multi-functional time and attendance application that incorporates a multi-tiered architecture. Written in Java, the application uses J2EE compliant technologies such as Java Servlets and Java Server Faces (JSF) and Java Facelets. Users connect to the system through an Apache web server.

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

This is N/A for VATAS; VATAS is not operated from multiple sites

3. Legal Authority and SORN

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

VATAS, under 5 CFR part 4501, Office of Personnel Management, provides a restricted-membership information interface and the data originates and remains within the financial systems and operations services of the VA. The data is not mined nor collected for any other purpose, in accordance with the system ISA/MOU. ISA/MOUs are used for the connections to/from VA entities, VATAS application provides required reports using restricted membership web interfaces and uses datasets from HRSMART, Defense Civilian Pay System (DCPS) and receives interface from Defense Finance and Accounting Service (DFAS). Personnel and Accounting Integrated Data System - VA (27VA047). The current SORN will be replaced with 208VA0478C, which is under review by VA Privacy Act Service.

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?

Personnel and Accounting Integrated Data System - VA (27VA047). The current SORN will be replaced with 208VA0478C, which is under review by VA Privacy Act Service.

D. System Changes

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

No, it cannot result in circumstances that require changes to business processes

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

No, it could not potentially result in technology changes

Section 1. Characterization of the Information

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

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

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

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

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

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

- ☒ Name
- ☒ Social Security Number
- ☐ Date of Birth
- ☐ Mother's Maiden Name
- ☐ Personal Mailing Address
- ☐ Personal Phone Number(s)
- ☐ Personal Fax Number
- ☐ Personal Email Address
- ☐ Emergency Contact Information (Name, Phone Number, etc. of a different individual)
- ☐ Financial Information
- ☐ Health Insurance Beneficiary Numbers Account numbers
- ☐ Certificate/License numbers*
- ☐ Vehicle License Plate Number
- ☐ Internet Protocol (IP) Address Numbers
- ☐ Medications
- ☐ Medical Records
- ☐ Race/Ethnicity
- ☐ Tax Identification Number
- ☐ Medical Record Number
- ☐ Gender
- ☐ Integrated Control Number (ICN)
- ☐ Military History/Service Connection
- ☐ Next of Kin
- ☒ Other Data Elements (list below)

- Work Email Address

<<Add Additional Information Collected But Not Listed Above Here (For Example, A Personal Phone Number That Is Used As A Business Number)>>
*Specify type of Certificate or License Number (e.g. Occupational, Education, Medical)

PII Mapping of Components (Servers/Database)

VATAS consists of **2 database servers'** key components (servers/databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by **VATAS** and the reasons for the collection of the PII are in the table below.

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

Internal Database Connections

Database Name of the information system collecting/storing PII	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
VAPRDP Oracle Database (#1)	Yes	Yes	Name, Work Email and SSN	Payroll Processing	Access control, authentication, configuration management, etc.
VAPRDR Oracle Database (#2)	Yes	Yes	Name, Work Email and SSN	Payroll Processing	Access control, authentication, configuration management, etc.

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?

Restricted membership-web access VATAS application manages all VA employee time and attendance functions, provides required reports using restricted membership web interfaces, and uses datasets from HRSMART, Defense Civilian Pay System (DCPS)and receives interface from Defense Finance and Accounting Service (DFAS).

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.

This is not applicable

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

VATAS has a reporting system

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?

Restricted membership web access VATAS application manages all VA employee time and attendance functions, provides required reports using restricted membership web interfaces, and uses datasets from HRSMART, and provides datasets to Defense Civilian Pay System (DCPS) for Defense Finance and Accounting Service (DFAS). We get datasets via FTP from HRSMART. We return datasets via sFTP to DCPS/DFAS for further processing. VATAS does not receive information from individuals.

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

NA for VATAS

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.

VATAS provides an information interface. The data originates and remains within the financial systems and operations services of the VA. Accuracy of transmitted and stored data is ensured via the use of checksum and appropriate encryption standards. The use of encryption standards protects the data from unauthorized access, deletion, addition, or modification.

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

This is NA for VATAS

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

VATAS, under 5 CFR part 4501, Office of Personnel Management, provides a restricted-membership information interface and the data originates and remains within the financial systems and operations services of the VA. The data is not mined nor collected for any other purpose, in accordance with the system ISA/MOU. ISA/MOUs are used for the connections to/from VA entities, VATAS application provides required reports using restricted membership web interfaces and uses datasets from HRSMART, Defense Civilian Pay System (DCPS) and receives interface from Defense Finance and Accounting Service (DFAS). Personnel and Accounting Integrated Data System - VA (27VA047). The current SORN will be replaced with 208VA0478C, which is under review by VA Privacy Act Service.

1.6 <u>PRIVACY IMPACT ASSESSMENT: Characterization of the information</u>

Consider the specific data elements collected and discuss the potential privacy risks and what steps, if any are currently being taken to mitigate those identified risks. (*Work with your System ISSO to complete this section)*

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

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

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

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

<u>Principle of Data Quality and Integrity:</u> 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: There is a risk that an unauthorized user could access the database and work email addresses or Social Security Numbers could be discovered.

Mitigation: The data used by VATAS is restricted to necessary datasets only and it is used only for the purpose of processing time and attendance functions. VATAS does not collect information directly from the individual. VATAS uses FIPS 140-2 acceptable encryption and checksums for data integrity and quality. Access to VATAS is restricted and authentication is inherited from the VA, as we utilize a BPE TIC direct fiber link from the VA network directly to the AWS Cloud. VATAS uses restricted membership interfaces to provide access only to authorized users to minimize and control access to adhere to the security principle of least privilege.

Section 2. Uses of the Information

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

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

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

Using datasets from HRSMART, Defense Civilian Pay System (DCPS), VATAS application manages all VA employee time and attendance functions and provides required reports using restricted membership web interfaces and receives interface from Defense Finance and Accounting Service (DFAS) as required to allow for payroll processing.
Name: used as identifier
Social Security Number: used as an identifier.
Work Email address: used as an identifier and alternate login when the VA directs us to turn off Single Sign-on (SSO)

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 data is not mined nor collected for any other purpose, in accordance with the system Interconnection Security Agreement (ISA) /Memorandum of Understanding (MOU)

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.

VATAS does not create or make available new or previously unutilized information about an 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?

The data is not mined nor collected for any other purpose, in accordance with the system ISA/MOU. All personnel complete and annually repeat VA rules of behavior and privacy training. Accuracy of transmitted and stored data is ensured via the use of checksum and appropriate encryption standards. The PIA and SORN are clear about the permitted uses of the information, as is the system ISA/MOU. Information contained in the system is restricted to minimum required to meet system objectives only. Administrative access to VATAS is limited to less than ten targeted, required administrative employees, their privilege level is given by manager approval only and is monitored by the security manager

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

SSN is encrypted at rest in database

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

All security controls for Moderate system are implemented. The team members undergo security awareness training on an annual basis

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?

VATAS has implemented role-based access with least privileges

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

VATAS has implemented appropriate Access Controls

2.4c Does access require manager approval?

VATAS has segregation of duties and requires manager approval

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

VATAS keep track of access logs

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

VATAS implements appropriate encryption standards for data at rest and in transmission

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

VATAS retains name, work email address and SSN.

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.*

VATAS archives both application server and database server audit logs. Per NARA standards, audit logs are retained for 6 years

3.3 Has the retention schedule been approved by the VA records office and the National Archives and Records Administration (NARA)?

An approved records schedule must be obtained for any IT system that allows the retrieval of a record via a personal identifier. The VA Records Officer will assist in providing a proposed schedule. The schedule must be formally offered to NARA for official approval. Once NARA approves the proposed schedule, the VA records officer will notify the system owner.
This question is related to privacy control DM-2, Data Retention and Disposal.

3.3a Are all records stored within the system of record indicated on an approved disposition authority?

VATAS archives both application server and database server audit logs. Per NARA standards (File #310-1, nara-records-schedule-list.pdf (archives.gov) https://www.archives.gov/about/records-schedule/chapter-0.3html#padmin), audit logs are retained for 6 years

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

VATAS retains all records indefinitely as per directions from VATAS Business Unit. (Business Unit POC - Walter, Elaine Division Chief, PHRSD, Financial Payroll Service (FPS)

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.

VATAS adheres to NIST SP 800-88 Guidelines for Media Sanitization standards for record destruction, refer to NIST SP 800-88 Guidelines for Media Sanitization for a media destruction flowchart giving the details of the process.

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.

VATAS application manages all VA employee time and attendance functions, provides required reports using restricted membership interfaces, and provides interface to Defense Civilian Pay System (DCPS) and receives interface from Defense Finance and Accounting Service (DFAS). The principles of minimization and data quality and integrity are inherited from those systems

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

Discuss the risks associated with the length of time data is retained and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

While we understand that establishing retention periods for records is a formal process, there are policy considerations behind how long a project keeps information. The longer a project retains information, the longer it needs to secure the information and assure its accuracy and integrity. The proposed schedule should match the requirements of the Privacy Act to keep the minimum amount of PII for the minimum amount of time, while meeting the Federal Records Act. The schedule should align with the stated purpose and mission of the system.

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

Principle of Minimization: Does the project retain only the information necessary for its purpose? Is the PII retained only for as long as necessary and relevant to fulfill the specified purposes?

Principle of Data Quality and Integrity: Has the PIA described policies and procedures for how PII that is no longer relevant and necessary is purged?
This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal.

Follow the format below:

Privacy Risk: VATAS Information kept longer than necessary potentially could be breached.

Mitigation: VATAS retains only the information necessary for the processing to support the required interfaces between HRSMART and DCPS to DFAS. The adherence to minimal usage is inherited from those systems. VATAS does not retain nor use any information nor is data mined nor collected for any other purpose, in accordance with the system ISA/MOU. VATAS archives only application server and database server audit logs. VATAS adheres to NIST SP 800-88 standards for record destruction.

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***
VATAS (VA Time and Attendance)	Limited datasets as needed to support payroll processing	Social Security Name Work email address	https
Corporate Data Warehouse (CDW)	Reporting based on information from multiple data sources	Social Security Name Work email address	Oracle GoldenGate
HRPAS	Limited datasets as needed to support payroll processing	Social Security Name Work email address	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: Allowing insecure connections from internal organizations and systems might lead to data being accessed by unauthorized or poorly authenticated users having access to the data >>

Mitigation: VATAS utilizes SSL certificates to protect the data that is transferred to, and from, VA employees. The DCPS interfaces utilize secure FTP (SFTP) and virtual private network (VPN) to transmit and receive data. VATAS retains only the information necessary for the processing to support the required interfaces. VATAS does not retain nor use any information nor is data mined nor collected for any other purpose, in accordance with the system ISA/MOU. Access to report interfaces is restricted to VA authenticated traffic only.

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

			be more than one)	
Defense Finance and Accounting Service (DFAS)	Limited datasets as needed to support payroll processing	• Social Security Number • Name • Work email Address	National ISA/MOU	sFTP over port 22 using SSL encryption
DCPS	Limited datasets as needed to support payroll processing	• Social Security Number • Name • Work email Address	National ISA/MOU	sFTP over port 22 using SSL encryption

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.

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: VATAS does not use personal information for secondary purposes. Before VATAS BPE TIC architecture was completed, and interface access was restricted to only VA-authenticated users, MEDCOI (Medical Community of Interest) had an interface access, but this is no longer in plan.

Mitigation: There is no external sharing of information outside of the VA Department

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.

VATAS does not collect information from the individual. VATAS receives only limited datasets to process time and attendance for payroll purposes. We receive and return limited datasets as detailed in the mapping in section 1.1. The control of notification of information use is inherited from the VA.

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

NA, does not apply to VATAS CLOUD

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.

NA, does not apply to VATAS CLOUD

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.

VATAS does not use system or personal information for secondary purposes. VATAS does not collect information from the individual. Control of notification of information use is inherited from the VA

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.

VATAS does not use system or personal information for secondary purposes. VATAS does not collect information from the individual. Control of notification of information use is inherited from the VA

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: VATAS does not use system or personal information for secondary purposes. VATAS does not collect information from the individual. Control of notification of information use is inherited from the VA.

Mitigation: VATAS does not use system or personal information for secondary purposes. VATAS does not collect information from the individual. Control of notification of information use is inherited from the VA.

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.***

VATAS does not use system or personal information for secondary purposes. VATAS does not collect information from the individual. Control of access of information use is inherited from the VA

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).

FSC FOIA Officer and if the Officer reaches out to VATAS the required information will be provided

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.

FSC FOIA Officer and if the Officer reaches out to VATAS the required information will be provided

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.

VATAS does not use system or personal information for secondary purposes. VATAS does not collect information from the individual. Control of correction of information use is inherited from the VA

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.

VATAS does not use system or personal information for secondary purposes. VATAS does not collect information from the individual. Control of correction of information use is inherited from the VA.

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.

VATAS does not use system or personal information for secondary purposes. VATAS does not collect information from the individual. Control of access to and notification of information use is inherited from the VA

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: VATAS does not use system or personal information for secondary purposes. VATAS does not collect information from the individual. Control of information use, access, redress and correction is inherited from the VA

Mitigation: VATAS does not use system or personal information for secondary purposes. VATAS does not collect information from the individual. Control of information use, access, redress and correction is inherited from the VA

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.

Access control is maintained in accordance with moderate information system control standards. User authentication is inherited from the VA because all user traffic is from within the VA network, because VATAS is a BPE with a direct fiber link from the VA network to our cages in CenturyLink DC5 (primary) and CH2 (alternate) datacenters. In addition, VATAS utilizes SSL certificates to protect the data that is transferred to, and from, VA interfaces. The DCPS interfaces utilize secure FTP (SFTP) and virtual private network (VPN) to transmit and receive data. The data is not mined nor collected for any other purpose, in accordance with the system ISA/MOU.

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?

NA for VATAS CLOUD

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.

NA for VATAS CLOUD

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.

Access control is maintained in accordance with moderate information system control standards. All contractors complete and annually renew VA rules of behavior and privacy training and sign NDAs as condition of employment

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 Security training is a requirement at VA, and all relevant VA-wide trainings are completed by all personnel annually. Personnel that will be accessing information systems must read and acknowledge their receipt and acceptance of the HIPAA, VA National Rules of Behavior (ROB) or VA Contractor's ROB prior to gaining access to any VA information system or sensitive information. The rules are included as part of the VA Privacy and Information Security Awareness training, which all personnel must complete via the VA's Talent Management System (TMS). After the user's initial acceptance of the Rules, the user must re-affirm their acceptance annually as part of the security awareness training. Acceptance is obtained via electronic acknowledgment and is tracked through the TMS system. VA users with access to protected health information must complete mandatory HIPAA Privacy training annually in TMS. In addition, all contractors complete and annually renew VA rules of behavior and privacy training.

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

8.4a If Yes, provide:

1. *The Security Plan Status:* Approved/Yes
2. *The System Security Plan Status Date:* Signed on 1/06/2023
3. *The Authorization Status:* Authorization to Operate (ATO)
4. *The Authorization Date:* 03/24/2022
5. *The Authorization Termination Date:* 03/23/2024
6. *The Risk Review Completion Date:* 01/10/2023
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* Moderate

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

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

N/A for VATAS CLOUD

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)*

VATAS is a customized COTS application that is hosted in the VAEC AWS Gov Cloud and IaaS

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.*

N/A to VATAS Cloud

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.

N/A to VATAS Cloud

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.

N/A to VATAS Cloud

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).

N/A to VATAS Cloud

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

ID	Privacy Controls
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: 2023.08.18 11:18:32 -05'00'

Privacy Officer, Mark Wilson

RITO-ANTHONY BRISBANE

Digitally signed by RITO-ANTHONY BRISBANE
Date: 2023.08.18 11:56:47 -05'00'

Information System Security Officer, Rito-Anthony Brisbane

JONATHAN LINDOW

Digitally signed by JONATHAN LINDOW
Date: 2023.08.18 12:45:04 -05'00'

Information System Owner, Jonathan 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).

HELPFUL LINKS:

Record Control Schedules:

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

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

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

National Archives (Federal Records Management):

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

VHA Publications:

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

VA Privacy Service Privacy Hub:

https://dvagov.sharepoint.com/sites/OITPrivacyHub

Notice of Privacy Practice (NOPP):

VHA Notice of Privacy Practices

VHA Handbook 1605.04: Notice of Privacy Practices