Privacy Impact Assessment for the VA IT System called:

OM FSC Data Analytics (DAS) Assessing Veterans Administration Corporate Office VACO Data Analytics Service (DAS) 161

Date PIA submitted for review:

11/12/24

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Kisha Brunson	Kisha.Brunson@va.gov	512-296-9379
Information System Security Officer (ISSO)	Ronald Murray	Ronald.Murray2@va.gov	512-460-5081
Information System Owner	Jonathan Lindow	Jonathan.Lindow@va.gov	737-802-9565

Abstract

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

The OM FSC Data Analytics Service (DAS) Assessing is an enterprise-level, integrated business intelligence and analytics (BI&A) platform characterized by a client/server architecture in which users across the Department of Veterans Affairs analyze data using platform clients. This application will provide high level business intelligence visualizations that are data agnostic, and provide information to support decision making at all levels of VA. This application will be accessible throughout the VA enterprise upon approval of VA Form 9957, Access Form for information systems. Designated Points of Contact (POC) per data product will use this application via web interface, after submitting an approved VA Form 9957 for access. The POC will access their data product at will and close their session when they have finished. DAS provides access to the statistical tools either through out-of-the-box availability or custom creation through use of open-source technologies (e.g., R, Python).

Overview

The overview is the most important section of the Privacy Impact Assessment (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 business purpose of the program, IT system, or technology and how it relates to the program office and agency mission?*

The IT system is platform owned by the FSC and supported by the (FSC) Office of Information and Technology. The DAS provides a suite of tools that assist business users in detecting trends, patterns, outliers, and non-obvious relationships using the information gathered from source systems. Through the system, a range of analytic capabilities are provided to analysts, business authors, or other approved users. Although the FSC DAS has the capability to data mine, the FSC does not currently use the system to data mine as defined under the Federal Agency Data Mining Reporting Act of 2007. The FSC DAS has access to data stored in source systems, with the potential to reach data associated with 21.1M Veterans and over 300,000 VA employees, and VA Contractors.

B. *Who is the owner or has control of the IT system or project? If the system has an eMASS entry, ensure this information matches with the eMASS entry.*

OM FSC Data Analytics (DAS) Assessing an integrated business intelligence and analytics (BI&A) platform operated by DAS and is owned by the FSC and supported by the (FSC) Office of Information and Technology.

2. Information Collection and Sharing

C. *Indicate the expected number of individuals whose information is stored in the system and include a brief description of the typical client or affected individual?*

Although DAS has the capability to data mine, the FSC does not currently use the system to data mine as defined under the Federal Agency Data Mining Reporting Act of 2007. FSC DAS has access to data stored in source systems, with the potential to reach data associated with 21.1M Veterans and over 300,000 VA Employees, and VA Contractors.

Check if Applicable	**Demographic of individuals**
☒	Veterans or Dependents
☒	VA Employees
☐	Clinical Trainees
☒	VA Contractors
☐	Members of the Public/Individuals
☐	Volunteers

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

DAS provides a suite of tools that assist business users in detecting trends, patterns, outliers, and non-obvious relationships using the information gathered from source systems. Through the system, a range of analytic capabilities are provided to analysts, business authors, or other approved users.

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

The following categories of analytic methods are provided by the platform: Statistical analysis: modeling and statistical tools that can help analysts discover patterns or generalizations in the data; the analysis can be used to produce models that can be used to identify similar patterns in other data or common characteristics among seemingly disparate data; analytic methods include forecasting, regression, General Linear Model (GLM) variants, optimization modeling and related approaches. Geospatial analysis: visualization tools that can display a set of events or activities on a map showing streets, distances, demographic borders, and related features. The types of analysis supported through geospatial modeling include a wide range of resource allocation applications as well as and compliance/oversight. Temporal analysis: visualization tools that can display events or activities in a timeline to help an analyst/user identify patterns or associations in the data. Temporal analytic methods can produce a time sequence of events that can be used to predict future activities or discover similar types of activities. Analytics dashboards and advanced interactive exploration: The DAS provides authorized users with the ability to interact with DAS-created or enabled dashboards in which users can filter information among a range of dimensions within the dashboard (e.g., space, time, organizational hierarchy, etc.). Further, the DAS provides access to the statistical tools either through out-of-the- box availability or custom creation through use of open-source technologies (e.g., R, Python). Information can be shared via PowerBI reports or data extracts to Financial Services Center, National Cemetery Administration, Office of Integrated Veteran Care, VA Corporate Travel and Charge Card Service, VA Office of Finance, VA Office of Integrity and Compliance, VA Central Office, Veteran Benefits Administration, Veteran Health Administration, and Office of Information Technology.

F. Are the modules/subsystems only applicable if information is shared?

No

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

The system is only operated in one site.

3. Legal Authority and System of Record Notices (SORN)

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

As an organizational element of the FSC, the Data Analytics Division and its supporting technologies are authorized and the system has the legal authority that permits the collection, use, maintenance and sharing of personally identifiable information (PII), under Title 5 USC 552a, Public Law 103-356 and Public Law 109-114, and applicable SORN131VA047:
https://www.govinfo.gov/content/pkg/FR-2023-09-15/pdf/2023-20052.pdf

H. *What is the SORN?*

As an organizational element of the FSC, the Data Analytics Division and its supporting technologies are authorized and the system has the legal authority that permits the collection, use, maintenance and sharing of personally identifiable information (PII), under Title 5 USC 552a, Public Law 103-356 and Public Law 109-114, and applicable SORN131VA047:
https://www.govinfo.gov/content/pkg/FR-2023-09-15/pdf/2023-20052.pdf

I. *SORN revisions/modification*

No revision/ modification need at this time

I. *If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval.*

No revision/ modification need at this time

4. System Changes

J. *Will the business processes change due to the information collection and sharing?*

☐ Yes
☒ No
if yes, <<ADD ANSWER HERE>>

K. *Will the technology changes impact information collection and sharing?*

☐ Yes
☒ No
if yes, <<ADD ANSWER HERE>>

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 Information 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
☒ **Full** Social Security Number
☒ **Partial** 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/Sex
☒ Integrated Control Number (ICN)
☒ Military History/Service Connection

☒ Next of Kin
□ Date of Death
□ Business Email Address
□ Electronic Data Interchange Personal Identifier (EDIPI) □ Other Data Elements (list below)

Other PII/PHI data elements: Employee ID, Geospatial Data, Veteran Sponsor Information, Travel Card Number, Beneficiary Information, Traveler ID

1.2 List 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?

DAS does not collect information from individuals. The system interfaces with financial systems that may contain sensitive information (e.g., U.S. Bank Def File for Account Holder Names).

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.

DAS retrieves data from source systems based upon the parameters defined by the DAS technical team, who defines how the data are retrieved for the DAS. DAS includes data from the Financial Management System (FMS), Integrated Funds Distribution Control Point Activity Accounting & Procurement (IFCAP) System, Electronic Contract Management System (eCMS), Concur Federal Travel System, Veterans Administration Time & Attendance System (VATAS) as well as from files/tables created and maintained within the Corporate Data Warehouse (CDW).

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

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

DAS, as a source of analytical information, provides authorized users with the ability to interact with DAS-created or enabled dashboards in which users can filter information among a range of dimensions within the dashboard (e.g., space, time, organizational hierarchy, etc.

1.3 Methods of information collection

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?

DAS collects data by directly connecting to the source system's database via a series of database queries and through use of native connectors; data are also received via secure electronic transmission (secure FTP), in accordance with the MOU/SLA.

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?

No OMB control number

1.4 Information checks for accuracy, and 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.

Data is checked for accuracy if used in an investigation. DAS staff may manually create, edit, or delete tags that relate disparate records; however, the DAS is not the original point of collection for the information in the reports/analytics it provides. The accuracy of the data analyzed in the DAS depends on the accuracy of the source system providing the information—source system stewards have responsibility for data accuracy and quality.

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?

DAS in not checking for data accuracy because DAS is not the originator or point of collection for the information in the products it provides.

1.5 Identify the specific legal authorities, arrangements, and agreements that 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*

A. Federal Acquisition Regulation (FAR), Part 13, 48 CFR part 13, and Public Law 93-579, section 7(b).
B. Title 40 U.S.C. § 1401 (3), Clinger-Cohen Act of 1996, which directs the development and maintenance of IT architectures by federal agencies to maximize benefits within the federal government.
C. Government Performance and Results Act of 1993, designed to improve federal program effectiveness, enhance Congressional decision-making, and strengthen internal controls.
D. Public Law 103-356 and Public Law 109-114.
E. Title 5 USC 552a.

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: *The collection ties with the purpose of the underlying mission of the organization and its enabling authority.*

Principle of Minimization: *The information is directly relevant and necessary to accomplish the specific purposes of the program.*

Principle of Individual Participation: *The program, to the extent possible and practical, collects information directly from the individual.*

Principle of Data Quality and Integrity: *VA policies and procedures must ensure that personally identifiable information is accurate, complete, and current.*
This 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:. PII/PHI of a veteran may not be relevant, accurate, compete, and/or current.

Mitigation: Users are granted role-based access to the system interconnections with DAS. Before gaining access to DAS, a user must submit a request for access that routes through supervisory and subject area owner channels. Systems administration and information security will have accessibility to user logs that allow identification of users. Coupled with the user access review process, routine and recurrent monitoring by information security and DAS application management will mitigate the potential for unauthorized access.

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 as personal identifier	Not used
Social Security Number	Used as personal identifier and to confirm person	Not used
Date of Birth	Used as personal identifier and to determine age	Not used
Mother's Maiden Name	Used as personal identifier and to confirm person	Not used
Personal Mailing Address	Used to enable dashboard/report to customers to contact individual (DAS doesn't contact individuals)	Not used
Personal Phone Number(s)	Used to enable dashboard/report to customers to contact individual (DAS doesn't contact individuals)	Not used
Personal Fax Number	Used to enable dashboard/report to customers to contact individual (DAS doesn't contact individuals)	Not used
Personal Email Address	Used to enable dashboard/report to customers to contact individual (DAS doesn't contact individuals)	Not used
Emergency Contact Information	Used to enable dashboard/report to customers to contact individual (DAS doesn't contact individuals)	Not used
Financial Information	Used to enable dashboard/report customers to provide financial transaction support to their clients	Not used

Health Insurance Beneficiary Numbers Account Numbers	Used to enable dashboard/report to customers to provide health insurance transaction support to their clients	Not used
Medical Records	Used to enable dashboard/report customers to provide medical support to their clients and to track their clients’ medical history	Not used
Race/Ethnicity	Used to enable dashboard/report customers to garner demographics data	Not used
Tax Identification Number	Used as personal identifier and to confirm person	Not used
Medical Record Number	Used as personal identifier and to confirm person	Not used
Gender	Used to enable dashboard/report customers to garner demographics data	Not used
Integrated Control Number (ICN)	Used for reporting purposes	Not used
Next of Kin	Used to enable dashboard/report customers to contact next of kin (DAS doesn’t contact individuals)	Not used
Other Data Elements (Employee ID)	Used as personal identifier and to confirm person	Not used
Other Data Elements (Geospatial Data)	Used to enable dashboard/report customers to garner geo-location data on their clients	Not used
Other Data Elements (Veteran Sponsor Info)	Used to enable dashboard/report customers to identify family member sponsors for eligibility	Not used
Other Data Elements (Travel Card Number)	Used to enable dashboard/report customers to provide financial transaction support to their clients	Not used
Other Data Elements (Beneficiary Info)	Used to enable dashboard/report customers to provide health insurance transaction support to their clients	Not used
Other Data Elements (Traveler ID)	Used to enable dashboard/report customers to	Not used

	provide financial transaction support to their clients	

2.2 Describe the types of tools 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?

DAS uses the following applications: Microsoft SQL Server Management Studio, and Microsoft Power BI desktop. The types of analysis performed by DAS depend upon the requirements established by the VA customer. These include, but are not limited to, advanced analytics, supporting compliance and fraud, waste, and abuse (FWA) analytics. The methods used include the full spectrum of approaches in FWA-from traditional rules-based to statistically based analyses. Specific examples of analytic methods employed include: • Development of machine learning algorithms to identify clusters of high-risk transactions in purchase cards • Outlier detection through a variety of statistical approaches • Development and application of matching algorithms • Use of largest subset and largest growth forensic tests.

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.

Output from analytic methods may include model coefficients, risk scores, goodness of fit (GOF)indicators, test statistics, p-values, and other relevant output. Program offices consume the results produced by the products enabled or developed by the DAS—the DAS does not change data insource systems because of the use of analytic methods.

2.3 How the information in the system is 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?

Data is encrypted, using a FIPS validated cryptographic module, at-rest and in-transit.

2.3b If the system is collecting, processing, or retaining Social Security Numbers, are there additional protections in place to protect SSNs? (refer to PTA question 3.8).

Role-Based Access Controls (RBAC) and the concept of least privilege are implemented in DAS. Business process approvals occur through the RBAC implementation, which also restrict who can access the PII, including Social Security Numbers.

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

Persons involved in the design, development, operation, or maintenance of any system of records, or maintaining any records goes through yearly required training provided by the VA through TMS. The Privacy office also conducts reviews of privacy changes during each major change in a system.

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?

Role-Based Access Controls (RBAC) and the concept of least privilege are implemented in DAS. Business process approvals occur through the RBAC implementation, which also restrict who can access the PII, including Social Security Numbers.

2.4b Are criteria, procedures, controls, and responsibilities regarding access documented? How are the documented, i.e. Policy, SOP, other. And where is this documentation located?

Contract and federal staff are required to take Privacy, HIPAA, and information security training annually in the VA’s Talent Management System (TMS). Access policies and procedures are determined by OI&T.

2.4c Does access require manager approval?

Yes

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

Yes

2.4e Who is responsible for assuring safeguards for the PII as identified in eMASS?

DAS personnel are trained and responsible for assuring safeguard for the PII.

Section 3. Retention of Information

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

3.1 What information is retained?

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

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, Medical Records, Race/Ethnicity, Tax Identification Number, Medical Record Number, Gender, Integrated Control Number (ICN), Next of Kin, Employee ID, Geospatial Data, Veteran Sponsor Info, Travel Card Number, Beneficiary Info, Traveler ID

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 https://www.archives.gov/records-mgmt/grs? This question is related to privacy control DM-2, Data Retention and Disposal.*

DAS is not the original point of collection for data—source system owners are responsible for information retention within the systems that DAS uses for analytics. Generally, records are retained as long as required per National Archivist and Records Administration (NARA) standards (Reference: GRS Schedule 1.1, Item #10). Retention length in SORN: "destroy 6 years after final payment or cancellation, but longer retention is authorized if required for business use."

3.3 The retention schedule 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. Please work with the system 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?

Each owning service is required to file plans identifying what records they are maintaining. Approved NARA GRS are identified, and specific retention guidelines are documented and followed in accordance with IAW VA Handbook 6300.1, Records Management Procedures.

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

Each owning service is required to file plans identifying what records they are maintaining. Approved NARA GRS are identified, and specific retention guidelines are documented and followed in accordance with IAW VA Handbook 6300.1, Records Management Procedures.
See: https://www.archives.gov/records-mgmt/grs.html

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

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

Electronic records are retained as long as required (GRS Schedule 1.1, Item #10), and are destroyed IAW NARA disposition instructions. Additionally, DAS follows Field Security Service (FSS) Bulletin #176 dated April 9, 2014, for Media Sanitization Program as well as FSS Standing Operating Procedures (SOP) MP-6, Electronic Media Sanitization. Information Technology Services/Database Administration has procedures to automate the destruction of media at the appropriate time based on published NARA and VA instructions. Internal Management ensures these procedures are enforced IAW FSC Directive 6300 and VA 6300.1 (Records Management).

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.

It is common to use hashing to mask PII or PHI in test and development environments. Pre-production and production environments communally do not mask PII or PHI but have controls in place such as role-based access and role level security.

<u>3.6 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 Privacy Officer (PO) 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: *The project retains only the information necessary for its purpose, additionally, the PII is retained only for as long as necessary and relevant to fulfill the specified purposes.*

Principle of Data Quality and Integrity: *The PIA should describe 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: There is a risk that the information maintained by the host systems will be retained for longer than is necessary to fulfill the VA mission. Records held longer than required are at greater risk of being unintentionally released or breached.

Mitigation: In addition to collecting and retaining only information necessary for fulfilling the VA mission, the disposition of data housed in host systems is based on standards developed by the National Archives Records Administration (NARA), which ensures that data are held for only as long as necessary. The Records Manager ensures data retention policies and procedures are followed, whereas the Privacy Officer, Information Security Officer, and Chief Information Officer monitor controls to mitigate any breaches of security and privacy.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

The following questions are intended to define the scope of information sharing/receiving/transmitting within VA.

PII Mapping of Components

4.1a **OM FSC Data Analytics (DAS) Assessing** consists of 161 key components (servers/databases/instances/applications/software/application programming interfaces (API)). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by **OM FSC Data Analytics (DAS) Assessing** and the reasons for the collection of the PII are in the table below.

Note: Due to the PIA being a public facing document, please do not include server names in the table. The first table of 3.9a 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
ADHOC ARVT CFO CPM_BIX CRM D3IMT DAS DBASysMaint DGT DMLSS EDI EFT_Matching FHS_Dashboard_Data FMP_EFTM FOS FSCContractData NAC PAYROLL PCARD PLO_LogOPS PLOBudget PLOOR TRAVEL VENDOR Vendor_File_BIX	Yes	Yes	• 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 • Medical Records • Race/Ethnicity • Tax Identification Number • Medical Record Number • Gender • Integrated Control Number (ICN) • Next of Kin • Other Data Elements (Employee ID)	Data Analysis and to enable dashboard/report customers to view necessary data for reporting.	Role based access granted through Active Directory controls, Least Privilege access controls, secured system account connections, data encryption at rest, data encryption in transit. HTTPS and TSL/SSL over communication

			- Other Data Elements (Geospatial Data) - Other Data Elements (Veteran Sponsor Info) - Other Data Elements (Travel Card Number) - Other Data Elements (Beneficiary Info) - Other Data Elements (Traveler ID)		
DBASysMaint SCCOP UDO	Yes	Yes	- 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 - Medical Records - Race/Ethnicity	Data Analysis and to enable dashboard/report customers to view necessary data for reporting.	Role based access granted through Active Directory controls, Least Privilege access controls, secured system account connections, data encryption at rest, data encryption in transit. HTTPS and TSL/SSL over communication.

			• Tax Identification Number • Medical Record Number • Gender • Integrated Control Number (ICN) • Next of Kin • Other Data Elements (Employee ID) • Other Data Elements (Geospatial Data) • Other Data Elements (Veteran Sponsor Info) • Other Data Elements (Travel Card Number) • Other Data Elements (Beneficiary Info) • Other Data Elements (Traveler ID)		

4.1b List internal organizations information is shared/received/transmitted, the information shared/received/transmitted, and the purpose, and how the information is transmitted.

NOTE: Question 3.9b (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

IT system and/or Program office. Information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List PII/PHI data elements shared/received/transmitted.***	***Describe the method of transmittal***
Financial Services Center, and related satellites	Oversight, compliance; descriptive and diagnostic analytics	• *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* • *Medical Records* • *Race/Ethnicity* • *Tax Identification Number* • *Medical Record Number* • *Gender* • *Integrated Control Number (ICN)* • *Next of Kin* • *Other Data Elements (Employee ID)* • *Other Data Elements (Geospatial Data)* • *Other Data Elements (Veteran Sponsor Info)* • *Other Data Elements (Travel Card Number)*	Consumer license through BI&A platform (VA internal web client). HTTPS

IT system and/or Program office. Information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List PII/PHI data elements shared/received/transmitted.***	***Describe the method of transmittal***
		• *Other Data Elements (Beneficiary Info)* • *Other Data Elements (Traveler ID)*	
National Cemetery Administration (NCA)	Oversight, compliance; operational improvement; descriptive and diagnostic analytics	• *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* • *Medical Records* • *Race/Ethnicity* • *Tax Identification Number* • *Medical Record Number* • *Gender* • *Integrated Control Number (ICN)* • *Next of Kin* • *Other Data Elements (Employee ID)* • *Other Data Elements (Geospatial Data)* • *Other Data Elements (Veteran Sponsor Info)* • *Other Data Elements (Travel Card Number)* • *Other Data Elements (Beneficiary Info)* • *Other Data Elements (Traveler ID)*	Consumer license through BI&A platform (VA internal web client). HTTPS

IT system and/or Program office. Information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List PII/PHI data elements shared/received/transmitted.***	***Describe the method of transmittal***
Integrated Veteran Care (IVC)	Oversight, compliance; descriptive, diagnostic, and predictive analytics	• *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* • *Medical Records* • *Race/Ethnicity* • *Tax Identification Number* • *Medical Record Number* • *Gender* • *Integrated Control Number (ICN)* • *Next of Kin* • *Other Data Elements (Employee ID)* • *Other Data Elements (Geospatial Data)* • *Other Data Elements (Veteran Sponsor Info)* • *Other Data Elements (Travel Card Number)* • *Other Data Elements (Beneficiary Info)* • *Other Data Elements (Traveler ID)*	Consumer license through BI&A platform (VA internal web client) HTTPS
VA Corporate Travel and Charge Card Service (CTCCS)	Oversight, compliance; descriptive, diagnostic,	• *Name* • *Social Security Number* • *Date of Birth* • *Mother's Maiden Name*	Consumer license through BI&A platform (VA internal

IT system and/or Program office. Information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List PII/PHI data elements shared/received/transmitted.***	***Describe the method of transmittal***
	and predictive analytics	• *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* • *Medical Records* • *Race/Ethnicity* • *Tax Identification Number* • *Medical Record Number* • *Gender* • *Integrated Control Number (ICN)* • *Next of Kin* • *Other Data Elements (Employee ID)* • *Other Data Elements (Geospatial Data)* • *Other Data Elements (Veteran Sponsor Info)* • *Other Data Elements (Travel Card Number)* • *Other Data Elements (Beneficiary Info)* • *Other Data Elements (Traveler ID)*	web client) HTTPS
VA Office of Finance (OF)	Oversight, compliance; descriptive, diagnostic, and predictive analytics	• *Name* • *Social Security Number* • *Date of Birth* • *Mother's Maiden Name* • *Personal Mailing Address* • *Personal Phone Number(s)* • *Personal Fax Number*	Consumer license through BI&A platform (VA internal web client) HTTPS

IT system and/or Program office. Information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT system*	*List PII/PHI data elements shared/received/transmitted.*	*Describe the method of transmittal*
		• *Personal Email Address* • *Emergency Contact Information (Name, Phone Number, etc. of a different individual)* • *Financial Information* • *Health Insurance Beneficiary Numbers Account Numbers* • *Medical Records* • *Race/Ethnicity* • *Tax Identification Number* • *Medical Record Number* • *Gender* • *Integrated Control Number (ICN)* • *Next of Kin* • *Other Data Elements (Employee ID)* • *Other Data Elements (Geospatial Data)* • *Other Data Elements (Veteran Sponsor Info)* • *Other Data Elements (Travel Card Number)* • *Other Data Elements (Beneficiary Info)* • *Other Data Elements (Traveler ID)*	
VA Office of Integrity and Compliance (OIC)	Oversight, compliance, risk identification and mitigation; descriptive, diagnostic, and predictive analytics	• *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*	Consumer license through BI&A platform (VA internal web client) HTTPS

IT system and/or Program office. Information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List PII/PHI data elements shared/received/transmitted.***	***Describe the method of transmittal***
		Number, etc. of a different individual) • *Financial Information* • *Health Insurance Beneficiary Numbers Account Numbers* • *Medical Records* • *Race/Ethnicity* • *Tax Identification Number* • *Medical Record Number* • *Gender* • *Integrated Control Number (ICN)* • *Next of Kin* • *Other Data Elements (Employee ID)* • *Other Data Elements (Geospatial Data)* • *Other Data Elements (Veteran Sponsor Info)* • *Other Data Elements (Travel Card Number)* • *Other Data Elements (Beneficiary Info)* • *Other Data Elements (Traveler ID)*	
VA Central Office (VACO)	Oversight, compliance, risk identification and mitigation; descriptive, diagnostic, and predictive analytics	• *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*	Consumer license through BI&A platform (VA internal web client) HTTPS

IT system and/or Program office. Information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List PII/PHI data elements shared/received/transmitted.***	***Describe the method of transmittal***
		• *Health Insurance Beneficiary Numbers Account Numbers* • *Medical Records* • *Race/Ethnicity* • *Tax Identification Number* • *Medical Record Number* • *Gender* • *Integrated Control Number (ICN)* • *Next of Kin* • *Other Data Elements (Employee ID)* • *Other Data Elements (Geospatial Data)* • *Other Data Elements (Veteran Sponsor Info)* • *Other Data Elements (Travel Card Number)* • *Other Data Elements (Beneficiary Info)* • *Other Data Elements (Traveler ID)*	
FSC Local/Satellite Payroll Offices	Oversight, compliance; descriptive and diagnostic analytics	• *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* • *Medical Records*	Consumer license through BI&A platform (VA internal web client) HTTPS

IT system and/or Program office. Information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List PII/PHI data elements shared/received/transmitted.***	***Describe the method of transmittal***
		• *Race/Ethnicity* • *Tax Identification Number* • *Medical Record Number* • *Gender* • *Integrated Control Number (ICN)* • *Next of Kin* • *Other Data Elements (Employee ID)* • *Other Data Elements (Geospatial Data)* • *Other Data Elements (Veteran Sponsor Info)* • *Other Data Elements (Travel Card Number)* • *Other Data Elements (Beneficiary Info)* • *Other Data Elements (Traveler ID)*	
Veteran Benefits Administration (VBA)	Oversight, compliance, risk identification and mitigation; descriptive, diagnostic, and predictive analytics	• *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* • *Medical Records* • *Race/Ethnicity* • *Tax Identification Number* • *Medical Record Number* • *Gender*	Consumer license through BI&A platform (VA internal web client) HTTPS

IT system and/or Program office. Information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List PII/PHI data elements shared/received/transmitted.***	***Describe the method of transmittal***
		• *Integrated Control Number (ICN)* • *Next of Kin* • *Other Data Elements (Employee ID)* • *Other Data Elements (Geospatial Data)* • *Other Data Elements (Veteran Sponsor Info)* • *Other Data Elements (Travel Card Number)* • *Other Data Elements (Beneficiary Info)* • *Other Data Elements (Traveler ID)*	
Veteran Health Administration (VHA)	Oversight, compliance, risk identification and mitigation; descriptive, diagnostic, and predictive analytics	• *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* • *Medical Records* • *Race/Ethnicity* • *Tax Identification Number* • *Medical Record Number* • *Gender* • *Integrated Control Number (ICN)* • *Next of Kin*	Consumer license through BI&A platform (VA internal web client) HTTPS

IT system and/or Program office. Information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List PII/PHI data elements shared/received/transmitted.***	***Describe the method of transmittal***
		• *Other Data Elements (Employee ID)* • *Other Data Elements (Geospatial Data)* • *Other Data Elements (Veteran Sponsor Info)* • *Other Data Elements (Travel Card Number)* • *Other Data Elements (Beneficiary Info)* • *Other Data Elements (Traveler ID)*	
Office of Information Technology (OIT)	Oversight, compliance, risk identification and mitigation; descriptive, diagnostic, and predictive analytics.	• *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* • *Medical Records* • *Race/Ethnicity* • *Tax Identification Number* • *Medical Record Number* • *Gender* • *Integrated Control Number (ICN)* • *Next of Kin* • *Other Data Elements (Employee ID)* • *Other Data Elements (Geospatial Data)*	Consumer license through BI&A platform (VA internal web client) HTTPS

IT system and/or Program office. Information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List PII/PHI data elements shared/received/transmitted.***	***Describe the method of transmittal***
		• *Other Data Elements (Veteran Sponsor Info)* • *Other Data Elements (Travel Card Number)* • *Other Data Elements (Beneficiary Info)* • *Other Data Elements (Traveler ID)*	

4.2 <u>PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure</u>

Discuss the privacy risks associated with the sharing of information within the VA network 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 in this section.).

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

Follow the format below:

<u>Privacy Risk:</u> There is a risk that DAS users may be able to access and use DAS system information to which they normally do not have access.

<u>Mitigation:</u> Users are granted role-based access to the system interconnections with DAS. Before gaining access to DAS, a user must submit a request for access that routes through supervisory and subject area owner channels. Systems administration and information security will have accessibility to user logs that allow identification of users. Coupled with the user access review process, routine and recurrent monitoring by information security and DAS application management will mitigate the potential for unauthorized use.

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 List the external organizations (outside VA) that information shared/received. and information shared/received, and the purpose, and how the information transmitted and what measures are taken to ensure it is secure.

The sharing of information outside the agency must be compatible with the original collection. The sharing must be covered by an appropriate routine use in a SORN. If not covered, 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 IT System or External Program Office information is shared/received with	***List the purpose of information being shared / received / transmitted***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted)***	***List agreements such as: Contracts, MOU/ISA, BAA, SORN. etc. that permit external sharing (can be more than one)***	***List the method of transmission and the measures in place to secure data***
N/A	N/A	N/A	N/A	N/A

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

If no External Sharing listed on the table above, ***(State there is no external sharing in both the risk and mitigation fields).***

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

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

Follow the format below:

Privacy Risk: As DAS does not share data with external organizations at this time, there are minimal to no privacy risks to the data maintained in the system.

Mitigation: The key mitigation to any privacy risk related to external sharing of VA data from DAS is that the system does not connect to or share with any external organizations or systems at this time. Should VA mission requirements establish the need for data sharing, the FSC will (a) modify this PIA and (b) use existing data sharing regulations/guidelines found within the VA (e.g., VHA Handbook 1080.01, VHA Directive 1080) to develop necessary agreements to mitigate privacy and security risks.

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 The notice provided to the individual before collection of the information. Please provide a copy and/or screen shot of a web notice of the notice as an Appendix-A 6.1 on the last page of the document. (A notice may include a posted privacy policy, a Privacy Act notice on forms, notice given to individuals by the sources system, or a system of records notice published in the Federal Register.) If notice was not provided, explain why.

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 Provide the Privacy Notice provided to the public by this system or any source systems. Include a copy of the notice in Appendix A of the PIA, the Federal Register citation, or Privacy Statement from collection of information such as forms or surveys.

DAS collects and integrates data from a multitude of sources. DAS and its supporting personnel do not interact directly with individuals to collect PII data, although DAS uses data containing PII found in other systems. As data are reutilized in accordance with the source system authority, no notification is necessary, as any data corrections will occur in the source system, not within DAS. Individuals, upon request, are referred to the source system sponsor or owner if questions arise with respect to relevant SORN stated usages and implementation within DAS.

6.1b If notice was not provided, explain why.

DAS collects and integrates data from a multitude of sources. DAS and its supporting personnel do not interact directly with individuals to collect PII data, although DAS uses data containing PII found in other systems. Therefore, DAS is covered by the notice of the source system.

6.1c Provide how the notice provided at the time of collection meets the purpose of use for this system.

DAS collects and integrates data from a multitude of sources. DAS and its supporting personnel do not interact directly with individuals to collect PII data, although DAS uses data containing PII found in other systems. Therefore, DAS is covered by the notice of the source system.

6.2 Do individuals have the opportunity and right to decline to provide information? If so, is a penalty or denial of service attached?

This question is directed at whether the person from or about whom information is collected can decline to provide the information and if so, whether a penalty or denial of service is attached. This question is related to privacy control IP-1, Consent, IP-2, Individual Access, and IP-3, Redress.

Individuals can decline to provide information in accordance with (IAW) system privacy notices and SORNs. DAS does not provide specific notice prior to the collection of information because DAS is not the original point of collection.

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

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

Individuals may not directly access their information in DAS. Individuals seeking access to their information should follow the directions in the source systems PIAs and relevant SORNs.

6.4 <u>PRIVACY IMPACT ASSESSMENT: Notice</u>

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

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

<u>Principle of Transparency:</u> This is referring to sufficient notice provided to the individual.

<u>Principle of Use Limitation:</u> The information used only for the purpose for which notice was provided either directly to the individual or through a public notice. The procedures in place must 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:

<u>Privacy Risk:</u> Veterans and other members of the public may not know that DAS exists or that the system collects, analyzes, and/or disseminates PII and other SPI about them.

Mitigation: FSC mitigates this risk by clarifying DAS role through this PIA and the SORNs covering the various systems interacting with DAS. Individuals, upon request, are referred to the source system owner or sponsor.

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 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 [VA Public Access Link-Home (efoia-host.com)](https://www.efoia-host.com) to obtain information about FOIA points of contact and information about agency FOIA processes.***

Individuals may not directly access their information in DAS. Individuals seeking access to their information should follow the directions provided in the source systems PIAs and SORNs. Individuals may request access to their information by submitting a Privacy Act request unless the information is covered by an appropriate exemption from one or more of the Privacy Act requirements. To obtain access to his or her information, the individual would have to make either a Freedom of Information Act or Privacy Act request. Individuals who are seeking information pertaining to them are directed to clearly mark the envelope and letter "Privacy Act Request." Within the text of the request, the subject of the record must provide his/her full name, date and place of birth, and notarized signature, and any other information that may assist in identifying and locating the record, and a return address.

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 not exempt from the access provisions of the Privacy Act.

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

The system is not a Privacy Act system.

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

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

DAS itself does not permit individuals to amend erroneous information. Individuals seeking to correct inaccurate or erroneous information should follow the instructions provided in the source system SORN. Requests must be in writing and adequately describe the specific information or records that need to be amended. This request must be submitted to the VA health care facility that maintains the record, or the System Manager of the source System of Record.

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.

Individuals wishing to correct their personal information (whether medical, education, benefits, claims, or otherwise) would follow the respective data owner's processes/procedures.

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.

Redress processes are defined in 7.1 and 7.2 in this PIA. DAS stores and transmits data but does not process or correct it. Veterans may correct information IAW guiding processes/procedures developed by the organization owning the system data.

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 Privacy Officer (PO) to complete all Privacy Risk questions in this section).*

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

Principle of Individual Participation: The individual must be provided with the ability to find out whether a project maintains a record relating to them.

Principle of Individual Participation: If access and/or correction is denied, then is the individual must be provided notice as to why the denial was made and how to challenge such a denial.

Principle of Individual Participation: The mechanism by which an individual is able to prevent information about them obtained for one purpose from being used for other purposes without their knowledge.
This question is related to privacy control IP-3, Redress.

Follow the format below:

Privacy Risk: Veterans may not be given an adequate opportunity to correct information that DAS processes.

Mitigation: The VA FSC does not claim any Privacy Act exemptions for DAS. Individuals may submit a redress request or appeal as stated in the VA Privacy Act regulations. Requests must be in writing and adequately describe the specific information or records that need to be amended. This request must be submitted to the VA health care facility that maintains the record, or the System Manager of the source System of Record.

Section 8. Technical Access and Security

The following questions are intended to describe technical safeguards and security measures. (Work with your ISSO to complete this section).

8.1 The procedures in place to determine which users may access the system, must be 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?

DAS enforces strict access controls. Only users with a 'need to know' are able to access the data and produce reports. As a new user is defined for DAS, roles are assigned. Each role has one or more profiles associated with it. The Separation of Duties concept for DAS is applied in accordance with VA policy and procedures. In addition, for management of DAS, different personnel staff DAS System Administrators and DAS ISO positions. All access requests and changes must be processed by at least two people. There are three roles available in DAS: • Analyst •Developer •Consumer. Of the three roles, the analyst and developer roles have the widest capability and can create, read, update and delete inside DAS. The consumer role has the most restrictive capability and can only read inside DAS. Read capability is further restricted to DAS products that are specifically requested and approved by the user's supervisor or program manager. Individuals having temporary access to DAS will undergo an extensive high-level Tier 2 background check and will be provided read access only to data tables created by DAS staff. Contractors who have read and write access to DAS complete a Tier 2 High Level background check and undergo Privacy and Information Security/Rules of Behavior training.

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?

Currently, users request access through supervisors, VAFSC security administration, and systems administration. Users submit a paper or electronic VA Form 9957 to access DAS. If the Form 9957 is electronic, the Online Form System (OFS) will be used to route the request to their supervisor, who will approve or disapprove. If disapproved, it will be returned to the requestor for further action, or no action depending on the reason for disapproval. If approved, the OFS system will route the 9957 to VAFSC security administration, which will subsequently transfer the 9957 to the CA Help desk system and generate a help desk ticket. The ticket is then routed to systems administration, which establishes the user's permission and grants access to DAS. If the VA Form 9957 submission is a manual/paper submission, the requestor will generate and print the Form 9957, and transmit it to their supervisor, using electronic means, or the post office. Upon receipt, the supervisor will approve or disapprove. If disapproved, it will be returned to the requestor for further action, or no action depending on the reason for disapproval. If approved, the supervisor will transmit the approved Form 9957 to VAFSC security administration using electronic means, or the post office. The admin will transfer the Form 9957 to the CA Help desk system and generate a help desk ticket. The ticket is then routed to systems administration, which adjusts the user's permission and establishes access to DAS. These requests are submitted for approved users (i.e., VA employees, contractors, and so on) and are processed through the appropriate approval processes and reviewed and approved by two people. Once access is granted, individuals can log into the system(s) through dual authentication, i.e., a PIV card with a complex password combination. Once inside the system, individuals are authorized to access information on a need-to-know basis. An audit trail will be used for all the users who access DAS System. Strict physical security control measures are enforced to ensure that disclosure to these individuals is also based on this same principle. Generally, VA file areas are locked after normal duty hours and the facilities are protected from outside access by the Federal Protective Service or other security personnel. Access by Office of Inspector General (OIG) staff conducting an audit, investigation, or inspection is coordinated directly with the Financial Services Center through the relevant staff office (e.g., Privacy Office, Financial Services Center, etc.). DAS is located at the VA Financial Services Center, 7600 Metropolis Drive, Austin, Texas 78744.

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.

There are three roles available in DAS: analyst, business author, and consumer. Of the three roles, the analyst role has the widest capability and can create, read, update and delete inside DAS. The business author role can read and update inside DAS; whereas the consumer role has the most restrictive capability and can only read inside DAS. Read capability is further restricted to DAS products that are specifically requested and approved by the user's supervisor or program manager. Individuals having temporary access to DAS will undergo an extensive high-level Tier 2 background check and will be provided read access only to data tables created by DAS staff. Contractors who have read and write access to DAS complete a Tier 2 High Level background check and undergo Privacy and Information Security/Rules of Behavior training.

8.2a. Will VA contractors have access to the system and the PII?

Yes

8.2b. What involvement will contractors have with the design and maintenance of the system?

VA contractors require access to the system to comply with performance work statement requirements. VA contractor access is required for development and/or consumption of DAS products based on their position inside the VA FSC. Contractors are employed by the Data Analytics Division in architectural, analytic, and programmatic roles and require full access to fulfill the terms of their contracts. Contractors not in the Data Analytics Division may require access in the consumer role to fulfill their duties in their contracted role. Clearance to access to DAS is determined at the time of hire, or the time of DAS product deployment. Access is controlled per 8.1 of this PIA.

8.2c. Does the contractor have a signed confidentiality agreement?

Yes, all contractors are required to sign non-disclosure agreements (NDAs) and necessary contractual requirements governing access and handling of VA data.

8.2d. Does the contractor have an implemented Business Associate Agreement for applicable PHI?

Yes, all contractors are required to have an implemented Business Associate Agreement. Additionally, contractors are cleared using the VA Background investigation process and obtain a Minimum Background Investigation.

8.2e. Does the contractor have a signed non-Disclosure Agreement in place?

If so, how frequently are contracts reviewed and by whom? Describe the necessity of the access provided to contractors to the system and whether clearance is required. If Privacy Roles and Responsibilities have been established to restrict certain users to different access levels, please describe the roles and associated access levels. Explain the need for VA contractors to have access to the PII. This question is related to privacy control AR-3, Privacy Requirements for Contractors, and Service Providers.

VA contractors require access to the system to comply with performance work statement requirements. VA contractor access is required for development and/or consumption of DAS products based on their position inside the VA FSC. Contractors are employed by the Data Analytics Division in architectural, analytic, and programmatic roles and require full access to fulfill the terms of their contracts. Contractors not in the Data Analytics Division may require access in the consumer role to fulfill their duties in their contracted role. Clearance to access to DAS is determined at the time of hire, or the time of DAS product deployment. Access is controlled per 8.1 of this PIA. Contracts are reviewed quarterly for performance purposes by upper management and the assigned contracting officers.

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.

All users are required to complete the following training items annually: VA Privacy and Information Security Awareness and Rules of Behavior Privacy and HIPAA Training. Additional training is required for specialized roles in DAS: Information Security Role-Based Training for Data Managers (WBT).

8.4 The Authorization and Accreditation (A&A) completed for the system.

8.4a If Yes, provide:

1. *The Security Plan Status:* complete in eMass.
2. *The System Security Plan Status Date:* 06/17/2024
3. *The Authorization Status: 1-year* ATO was granted
4. *The Authorization Date:* November 1, 2024
5. *The Authorization Termination Date:* November 1, 2025
6. *The Risk Review Completion Date:* 11/02/2023
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. ***(Refer to question 1.8 of the PTA)***

DAS uses VA Enterprise Cloud

9.2 Does the contract with the Hosting 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 3.3.1 of the PTA)*** *This question is related to privacy control AR-3, Privacy Requirements for Contractors, and Service Providers.*

Yes

9.3 Will the CSP collect any ancillary data and if so, who has ownership over the ancillary data?

Per NIST 800-144, cloud providers hold significant details about the accounts of cloud consumers that could be compromised and used in subsequent attacks. Ancillary data also involves information the cloud provider collects or produces about customer-related activity in the cloud. It includes data collected to meter and charge for consumption of resources, logs and audit trails, and other such metadata that is generated and accumulated within the cloud environment.

This question is related to privacy control DI-1, Data Quality.

No

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

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

Yes, because this is within VAEC.

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).*

No

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

Signature of Responsible Officials

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

KISHA BRUNSON Digitally signed by KISHA BRUNSON
Date: 2024.11.25 13:20:22 -06'00'

Privacy Officer, Kisha E. Brunson

RONALD MURRAY Digitally signed by RONALD MURRAY
Date: 2024.11.25 13:41:34 -06'00'

Information System Security Officer, Ronald Murray

JONATHAN LINDOW Digitally signed by JONATHAN LINDOW
Date: 2024.11.25 13:14:59 -06'00'

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; screen shot of a website collection privacy notice).

Corporate Travel and Charge Cards -VA (131VA047).

https://www.govinfo.gov/content/pkg/FR-2023-09-15/pdf/2023-20052.pdf

HELPFUL LINKS:

Records Control Schedule 10-1 (va.gov)

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 Directive 1605.04
IB 10-163p (va.gov)