



Privacy Impact Assessment for the VA IT System called:

Federal Tax Information (FTI) Simple Object Access Protocol (SOAP)  
**Benefits, Appeals, and Memorials (BAM)**  
**Office of Information Technology (OIT)**

Date PIA submitted for review:

October 14, 2021

System Contacts:

*System Contacts*

	Name	E-mail	Phone Number
Privacy Officer	<i>Simon Caines</i>	<i>Simon.Caines@va.gov</i>	<i>202-461-9468</i>
Information System Security Officer (ISSO)	<i>Joseph Guillory</i>	<i>Joseph.Guillory@va.gov</i>	<i>510-637-6014</i>
Information System Owner	<i>Gary Dameron</i>	<i>Gary.Dameron2@va.gov</i>	<i>202-492-1441</i>

## Abstract

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

Benefits Integration Platform (BIP) provides a container-based application platform in VA Enterprise Cloud (VAEC) AWS in which VA benefits, appeals, and memorials (BAM) and Federal Tax Information (FTI) applications can be hosted. The Federal Tax Information (FTI) Simple Object Access Protocol (SOAP) service is hosted on the platform and passes Federal Tax Information (FTI) information provided by the Internal Revenue Service (IRS) to the VA for use in determining award eligibility for claimants. The FTI SOAP is a tenant of the FTI Secure Enclave environment that implements the safeguards necessary for housing FTI in the cloud. FTI SOAP will ingest documents to the FTI File Repository. This application will not collect or store information but will direct documents to the FTI File Repository. The system, in use of the data, will be used to decommission several legacy Veterans Benefits Administration (VBA) systems and enable the Pension Automation system to implement an Application Programming Interface (API) to make income eligibility determinations. The system has been approved by the Internal Revenue Service (IRS) Office of Safeguards (memo FD698-FED-AWS GovCloud-L-031020) as adequately implementing the safeguards outlined in IRS Publication 1075 and in accordance with Internal Revenue Code §6103(p)(4).

## 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:*

- *The IT system name and the name of the program office that owns the IT system.*
- *The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission.*
- *Indicate the ownership or control of the IT system or project.*
- *The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.*
- *A general description of the information in the IT system and the purpose for collecting this information.*
- *Any information sharing conducted by the IT system. A general description of the modules and subsystems, where relevant, and their functions.*
- *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.*
- *A citation of the legal authority to operate the IT system.*
- *Whether the completion of this PIA will result in circumstances that require changes to business processes*
- *Whether the completion of this PIA could potentially result in technology changes*
- *If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval? If the system is using cloud technology, does the SORN for the system cover cloud usage or storage?*

The Benefits Integration Platform (BIP) is owned, built, and managed by the benefits, appeals, and memorial (BAM) Program office in the Office of Information Technology (OIT). The FTI SOAP is a tenant of the FTI Secure Enclave environment that implements the safeguards necessary for housing FTI in the cloud. Benefits Integration Platform (BIP) hosts minor applications in support of the BAM Program office mission to serve Veterans and their families through various services offered. As part of the BIP accreditation boundary, the Federal Tax Information (FTI) SOAP ... provides a safeguarded repository to store FTI data to be used in claims processing such that several legacy systems may be decommissioned, including the Veterans Service Network (VETSNET) Modern Awards Processing-Development (MAP-D) and AWARDS applications along with the Legacy Document Repository component of Virtual VA. The Federal Tax Information (FTI) File SOAP ... Benefits Integration Platform (BIP) is owned, built, and managed by the benefits, appeals, and memorial (BAM) Program office in the Office of Information Technology (OIT). BIP hosts minor applications who will maintain their own Privacy documentation which will vary in information stored, clients, and affected individuals. VA Business Stakeholders of the BIP minor applications have ownership rights over data. In the SOAP no information on individuals is stored. The SOAP service will pass FTI data to support the pension claims process. FTI documents may include PII in the form of Social Security Number, address, name and financial information for Veterans and dependents. Benefits Integration Platform (BIP) provides a container-based application platform in VAEC AWS in which VA benefits, appeals, and memorial (BAM) and Federal Tax Information (FTI) applications can be hosted. The platform leverages Red Hat OpenShift and Kubernetes clusters for container management and orchestration, which allows teams to develop, scale, and deliver modern, secure, and properly segmented (from a storage, network, and compute perspective) applications in a multi-tenant environment. The AWS Virtual Private Clouds (VPCs) within BIP are sequentially peered to allow connectivity between VPCs, which supports the promotion of container images from lower VPCs to higher VPCs. The peering is essential for DevOps and Agile methodologies and is locked down to only allow container images to be mirrored between registries in each VPC. BIP also leverages a suite of TRM approved COTS tools (e.g. Jenkins, SonarQube, Vault, Nexus, Consul) to help development teams deliver quickly and effectively. In addition, BIP, as a General Support Systems (GSS), will further support VA minor application tenants by constraining the controls necessary for applications hosted on the platform. Minor applications and application programming interfaces (APIs) hosted on BIP Assessing and Secure Enclave on VAEC AWS include but are not limited to Vet Services Awards, Vet Services Ratings, Beneficiary and Fiduciary Field System(BFFS)/Veterans Benefit Management System (VBMS) Fiduciary, BIP Reference Person, Benefits Processing Data Service (BPDS), Benefits Security Services (BSS), Contention Classification Predictive Service (CCPS), Claim Automation Processor, Notes API, Veterans Benefit Management System (VBMS) Users API, Veteran API, Vet Services Claims, Compensation and Pension User Interface, Data Synchronization, Document Generator (DocGen), Enterprise Management Payment Workload and Reporting (eMPWR), FAS Notes, VBMS Transfer, Exam Destination, Exam Management, Fiduciary Service, FTI Capture, FTI File Repo, FTI Simple Object Access Protocol (SOAP), Integrated Benefits Services (IBS), Memorial Benefits Management System (MBMS), Package Manager (Pac Man), Pension Automation, Records Research Center (RRC), VASRD, VBMS Correspondence (VBMS-C), and Veteran Enterprise File Services (VEFS). BIP Assessing and the SOAP is operated in a single Region of the VA Enterprise Cloud (VAEC) in Amazon Web Services (AWS) GovCloud, deployed across three Availability Zones. Security and privacy data held by a cloud provider is still required to meet the requirements under the privacy act. Federal agencies are required to identify and assess the risk to their PII, and to ensure security controls are implemented to provide adequate safeguards. Section C MM. of the contract references OMB Memorandum "Security Authorization of Information Systems in Cloud Computing Environments" FedRAMP Policy Memorandum. VA

Enterprise Cloud Solutions group partnered with Amazon Web Services (AWS) a FedRAMP provider to offer VA programs the opportunity to host cloud applications. The production environment is hosted in AWS under VA Enterprise Cloud Solutions Office (ECSO) General Support System (GSS) and accredited as FISMA “HIGH” categorization. Custody and ownership of PII and PHI are solely the responsibility of the VA as a tenant of AWS, in accordance with VA policy and NIST 800-144. Both AWS and the VA have a tremendous interest in maintaining security of PII and PHI, including (but not limited to) HIPAA Enforcement Rule of 2006, HIPAA Omnibus, and HITECH. AWS is responsible for physical security, infrastructure security, network, and communications for the facility. VA is responsible for the maintaining application, data, and system security for the program. VA is the sole owner of all data stored within the system. The contract outlines Management of Security and Privacy Incidents in accordance with VA Handbook 6500.2. Based on determinations of independent risk analysis, the Contractor shall be responsible for paying to VA liquidated damages for affected individuals to cover the cost of providing credit protection services to affected individuals. CSPs are required to meet the same requirements when operating on behalf of the federal government. The Secure Enclave has been approved by the Internal Revenue Service (IRS) Office of Safeguards (memo FD698-FED-AWS GovCloud-L-031020) as adequately implementing the safeguards outlined in IRS Publication 1075 and in accordance with Internal Revenue Code §6103(p)(4). Legal authority for Federal Tax Information, to include identity information, be shared between Department of the Treasury/IRS and VA is codified in Internal Revenue Code §6103(l)(7), with identity information codified in §6103(b)(6). The ISA/MOU governing the information exchange between IRS and VA is codified in DART 52. As for the Veteran eFolder upon which FTI documents will be available within, the Secretary of Veterans Affairs established guidelines pursuant to the authorities in and requirements of Title 38, United States Code, section 81 11 (38 U.S.C. 5811 I), titled "Sharing of Department of Veterans Affairs and Department of Defense Health Care Resources," and the authorities contained under Title 10, United States Code, section 1104 (10 U.S.C. 1104), titled "Sharing of Resources with the Department of Veterans Affairs," which incorporates Title 31, United States Code, section 1535 (31 U.S.C. 51 535), titled "Agency Agreements," also known as the "Economy Act." These guidelines assist in the implementation of these statutes. Completion of this PIA will not result in circumstances requiring changes to business processes. Completion of this PIA is not anticipated to result in technology changes. The System of Record Notice (SORN) “VA Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records – VA” 58VA21/22/28 (February 14, 2019). This SORN can be found online at <https://www.govinfo.gov/content/pkg/FR-2019-02-14/pdf/2019-02315.pdf>

## 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://vawww.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:

- |  |   |  |
|--|---|--|
| <input checked="" type="checkbox"/> Name   | <input type="checkbox"/> Health Insurance Beneficiary Numbers   | <input type="checkbox"/> Integration Control Number (ICN)                  |
| <input checked="" type="checkbox"/> Social Security Number   | Account numbers   | <input type="checkbox"/> Military History/Service Connection               |
| <input checked="" type="checkbox"/> Date of Birth  | <input type="checkbox"/> Certificate/License numbers            | <input type="checkbox"/> Next of Kin                                       |
| <input type="checkbox"/> Mother's Maiden Name  | <input type="checkbox"/> Vehicle License Plate Number           | <input type="checkbox"/> Other Unique Identifying Information (list below) |
| <input checked="" type="checkbox"/> Personal Mailing Address   | <input type="checkbox"/> Internet Protocol (IP) Address Numbers |  |
| <input checked="" type="checkbox"/> Personal Phone Number(s)   | <input type="checkbox"/> Current Medications                    |  |
| <input checked="" type="checkbox"/> Personal Fax Number  | <input type="checkbox"/> Previous Medical Records               |  |
| <input checked="" type="checkbox"/> Personal Email Address   | <input type="checkbox"/> Race/Ethnicity                         |  |
| <input checked="" type="checkbox"/> Emergency Contact Information (Name, Phone Number, etc. of a different individual) | <input checked="" type="checkbox"/> Tax Identification Number   |  |
| <input checked="" type="checkbox"/> Financial Account Information  | <input type="checkbox"/> Medical Record Number                  |  |
|  | <input type="checkbox"/> Gender                                 |  |

Benefit Information  
Relationship to Veteran

**PII Mapping of Components**

**The FTI SOAP service** consists of **1** key component (databases) FTI SOAP Web Service. Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by FTI SOAP service and the reasons for the collection of the PII are in the table below.

## PII Mapped to Components

**Note:** Due to the PIA being a public facing document, please do not include the server names in the table.

### PII Mapped to Components

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
FTI SOAP Web Service	Yes	No	FTI documents and data have Veteran PII as provided by the IRS. This may include: SSN, address, name, email address, date of birth, contact numbers, tax identification numbers, and financial information for both	Eligibility determinations within the claims processing lifecycle.	Safeguards in accordance with IRS Publication 1075 will be implemented. In accordance with IRC §6103(p)(4) restrictions were certified by IRS as acceptable in memo FD698-FED-AWS GovCloud-L-031020 Approval from IRS that the solution will provide adequate safeguards was granted.

## 1.2 What are the sources of the information in the system?

*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?*

*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 1.3 indicate why the system is using this source of data.*

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

*This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.*

BIP Minor Applications manage their own information sources of data. In the current process FTI documents are captured at 3 Regional offices, Milwaukee, Philadelphia, and St. Paul. In the Secure Enclave, Veteran Service Representatives (VSRs) processing pension claims sometimes use FTI data to make income eligibility determinations for Veteran benefits.

### **1.3 How is the information collected?**

*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 technology used in the storage or transmission of information in identifiable form?*

*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.*

*This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.*

BIP Minor Applications manage their information collections processes. In the SOAP, FTI information is provided directly from IRS or through a subsidiary at the Social Security Administration (SSA) and is accessible in the VETSNET Share application. From Share, users will upload documents to the FTI Secure Enclave.

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

*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.*

*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 question is related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.*

Not applicable. Information is not retained in the SOAP Service.

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

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

*This question is related to privacy control AP-1, Authority to Collect*

The System of Record Notice (SORN) "VA Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records – VA" 58VA21/22/28 (February 14, 2019). This SORN can be found online at <https://www.govinfo.gov/content/pkg/FR-2019-02-14/pdf/2019-02315.pdf> 5 U.S.C. § 552a, Freedom of Information Act of 1996, As Amended By Public Law No. 104---231, 110 Stat. 3048 5 U.S.C. § 552a, Privacy Act of 1974, As Amended IRS memo FD698-FED-AWS GovCloud-L-031020. A current record of VA Sorns can be found at [https://www.oprm.va.gov/docs/Current\\_SORN\\_List\\_10\\_19\\_2021.pdf](https://www.oprm.va.gov/docs/Current_SORN_List_10_19_2021.pdf).

For the Secure Enclave, legal authority for Federal Tax Information, to include identity information, be shared between Department of the Treasury/IRS and VA is codified in Internal Revenue Code §6103(l)(7), with identity information codified in §6103(b)(6). The ISA/MOU governing the information exchange between IRS and VA is codified in DART 52.

As for the Veteran eFolder in Virtual VA (VVA) within which FTI documents will be available, the Secretary of Veterans Affairs established guidelines pursuant to the authorities in and requirements of Title 38, United States Code, section 81 11 (38 U.S.C. 5811 I), titled "Sharing of Department of Veterans Affairs and Department of Defense Health Care Resources," and the authorities contained under Title 10, United States Code, section 1104 (10 U.S.C.5 1104), titled "Sharing of Resources 31with the Department of Veterans Affairs," which incorporates Title 31, United States Code, section 1535 (31 U.S.C. 51 535), titled "Agency Agreements," also known as the "Economy Act." These guidelines assist in the implementation of these statutes.

### **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.*

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

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



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

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

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

Follow the format below when entering your risk assessment:

**Privacy Risk:** FTI SOAP processes PII intakes the PII and transfers to another system.

**Mitigation:** FTI SOAP uses encrypted communication received and sends data to FFR. No PII is stored in SOAP, so it does not risk necessary storage of PII at REST

## 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.*

VA provides a notice on the VA website that generally describes purposes for which PII may be collected, used, maintained, and shared for individuals doing business with VA benefits offices, VA executive offices, VHA facilities, and National Cemeteries.

FTI information as uploaded by users from use in income eligibility decisions will be stored along with letters sent to claimants that contain FTI data in the secure enclave. PII data as collected is used during the claims process to verify the identity of the claimant and Veteran.

Each use is documented below:

- Name - Used to identify the claimant or Veteran.
- Social Security Number - May be supplied by the IRS to uniquely identify the claimant or Veteran.
- Date of Birth - May be supplied by the IRS to uniquely identify the claimant or Veteran.
- Personal Mailing Address – May be included in Tax Return information provided by IRS. Also, will be included in FTI letters to the claimant or Veteran.

- Personal Phone Number(s) - May be included in Tax Return information provided by IRS.
- Personal Fax Number - May be included in Tax Return information provided by IRS.
- Personal Email Address - May be included in Tax Return information provided by IRS.
- Emergency Contact Information - May be included in Tax Return information provided by IRS.
- Financial Account Information – Supplied by the IRS to make income eligibility determinations within the Pension claims process.
- Tax Identification Number - May be supplied by the IRS to uniquely identify the claimant or Veteran.

## **2.2 What types of tools are used to analyze data and what type of data may be produced?**

*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.*

*If the system creates or makes available new or previously unutilized information about an individual, explain what will be done with the newly derived information. Will it be placed in the individual's existing record? Will a new record be created? Will any action be taken against or for the individual identified because of the newly derived data? If a new record is created, will the newly created information be accessible to Government employees who make determinations about the individual? If so, explain fully under which circumstances and by whom that information will be used.*

*This question is related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information*

SOAP does not perform any kind of data analysis or run analytic task.

## **2.3 How is the information in the system secured?**

*2.3a What measures are in place to protect data in transit and at rest?*

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

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

*This question is related to security and privacy controls SC-9, Transmission Confidentiality, and SC-28, Protection of Information at Rest*

The BIP Platform protects the confidentiality and integrity of the transmitted information within the system boundary. BIP Platform utilizes Amazon Elastic Block Storage (EBS) for platform component storage, including platform operational state from the distributed state model, as well as

for log files and log aggregators that could contain PII/PHI from BIP minor applications. Amazon EBS provides encryption of the volumes.

**2.4 PRIVACY IMPACT ASSESSMENT: Use of the information. How is access to the PII determined? Are criteria, procedures, controls, and responsibilities regarding access documented? Does access require manager approval? Is access to the PII being monitored, tracked, or recorded? Who is responsible for assuring safeguards for the PII?**

*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.*

VA Handbook 6500.2, Management of Breaches Involving Sensitive Personal Information establishes procedures for VA management of breaches involving VA Sensitive Personal Information

(SPI). The Handbook implements 38 U.S.C. §§ 5721-28 and 38 C.F.R. §§ 75.111-119; section 13402 of the Health Information Technology for Economic and Clinical Health (HITECH) Act (codified at 42 U.S.C. § 17932) and the Health Insurance Portability and Accountability Act (HIPAA) Breach Notification Rule at 45 C.F.R. §§ 164.400-414; the Privacy Act of 1974; and Office of Management and Budget (OMB) Memorandum 07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information.

The Agency Data Breach Core Team (DBCT) is the deciding group on credit monitoring services and notifications. They work with the facility to receive input and report on all privacy related breaches as well as those that fall under HIPAA/HITECH.

Breach management is part of the overarching incident management process designed to mitigate risk. The incident management process contains four main areas: (1) Incident Preparation; (2) Incident Detection, Reporting, and Analysis; (3) Corrective/Mitigation Action; and (4) Post-Incident Activity.

In the secure enclave, access to the PII is determined by authentication and authorization mechanisms implemented in the Virtual VA (VVA) system. The VVA PIA is maintained by the VVA Project Manager and can be obtained through him. Relevant excerpt from the VVA PIA below:

All employees with access to Veteran's information are required to complete the mandatory VA Privacy and Information Security Awareness training and Rules of Behavior annually. Disciplinary actions, depending on the severity of the offense, include counseling, loss of access, suspension and possibly termination.

Individual users are given access to Veteran's data through the issuance of a user ID and password and using a Personal Identity Verification (PIV) card. This ensures the identity of the user by requiring two-factor authentication. The user's ID limits the access to only the information required to enable the user to complete their job.

## **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*

Not applicable: SOAP does not collect and retain any of the information from question 1.1 The purpose of SOAP is to ingest documents into FFR.

### **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. 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. If the system is using cloud technology, will it be following the NARA approved retention length and schedule?*

*The VA records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented. This question is related to privacy control DM-2, Data Retention and Disposal.*

Not applicable

### **3.3 Has the retention schedule been approved by the VA records office and the National Archives and Records Administration (NARA)? If so please indicate the name of the records retention schedule.**

*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.*

Information retention requirements are governed by the Virtual VA (VVA) system from which FTI documents are accessed. The VVA PIA is maintained by the VVA PM and can be obtained through him. Relevant excerpt from the VVA PIA below:

VBA Records Management, Records Control Schedule VB-1, Part 1, Section VII as authorized by NARA

Compensation, Pension and Vocational Rehabilitation, Records Control Schedule VB-1 Part 1 Section XIII as authorized by NARA

Education – Regional Processing Office, Record Control Schedule VB-1, Part 1, Section VII as authorized by NARA

### **3.4 What are the procedures for the elimination of SPI?**

*Explain how records are destroyed or eliminated at the end of the 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 media sanitization, when the records are authorized for destruction (or upon system decommission), will be carried out in accordance with VA Handbook 6500 VA Cybersecurity Program. Paper documents are destroyed to an unreadable state in accordance with the Department of Veterans' Affairs VA Directive 6371, (October 29, 2010), [Department of Veterans' Affairs VA Directive 6371](#), Electronic data and files of any type, including Protected Health Information (PHI), Sensitive Personal Information (SPI), Human Resources records, and more are destroyed in accordance with the Department of Veterans' Affairs Directive 6500, VA Cybersecurity Program (February 24, 2021), [Directive 6500 24 Feb 2021.pdf \(va.gov\)](#). When required, this data is deleted from their file location and then permanently deleted from the deleted items, or Recycle bin. Magnetic media is wiped and sent out for destruction per VA Handbook 6500.1. Digital media is shredded or sent out for destruction per VA Handbook 6500.1. Additionally, this system follows Field Security Service (FSS) Bulletin #176 dated April 9, 2014 for Media Sanitization Program, SOPs - FSS - All Documents as well as FSS Standard Operating Procedures (SOP) MP-6 Electronic Media Sanitization.

### **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. Have policies and procedures been developed to minimize the use of PII for testing, training, and research?*

*This question is related to privacy control DM-3, Minimization of PII Used in Testing, Training and Research*

PII passed through the SOAP service is not used for research, training, or testing.

### **3.6 PRIVACY IMPACT ASSESSMENT: Retention of information**

*Discuss the risks associated with the length of time data is retained and what steps, if any, are currently being taken to mitigate those identified risks.*

*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:** As described herein, support systems retain information until that work in progress is completed and data is committed to master systems and records. The master systems retain data on a permanent basis (beyond the actual death of the Veteran). If a master system is to be deactivated, critical information is migrated to the new system and the old system along with associated data is archived according to the application disposition worksheet. As such, SPI, PII or PHI may be held for long after the original record was required to be disposed. This extension of retention periods increases the risk that SPI may be breached or otherwise put at risk.

**Mitigation:** User access is not provided by VVA but by the ePAS process. The following are true of all VA information system users:

All employees with access to Veteran's information are required to complete the mandatory VA Privacy and Information Security Awareness training and Rules of Behavior annually.

Disciplinary actions, depending on the severity of the offense, include counseling, loss of access, suspension and possibly termination. Individual users are given access to Veteran's data through the issuance of a user ID and password, and by the use of a Personal Identity Verification (PIV) card. This ensures the identity of the user by requiring two-factor authentication. The user's ID limits the access to only the information required to enable the user to complete their job.

VVA does not create, adjust, or make documents in any way, but is simply a repository for other systems. If a document is submitted to VVA as redacted, it is input as redacted.

## 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

<i>List the Program Office or IT System information is shared/received with</i>	<i>List the purpose of the information being shared /received with the specified program office or IT system</i>	<i>List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system</i>	<i>Describe the method of transmittal</i>
VirtualVA	VirtualVA	FTI documents may include: Social Security Number, address, name and financial information.	Encrypted SOAP transfer

<i>List the Program Office or IT System information is shared/received with</i>	<i>List the purpose of the information being shared /received with the specified program office or IT system</i>	<i>List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system</i>	<i>Describe the method of transmittal</i>
Benefits Integration Platform	VBMS	FTI documents may include: Social Security Number, address, name and financial information.	Secure iframe temporary file access that requires authentication

#### **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.*

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

Follow the format below:

**Privacy Risk:** The sharing of data is between VA systems is necessary to support the goals and purpose of the system. However, there is a risk that the data could be shared with an inappropriate VA organization which would potentially impact privacy.

**Mitigation:** The PII/PHI that is ingested through the SOAP service is encrypted. All employees/contractors with access to Veterans' information are required to complete the VA Privacy and Information Security Awareness training and Rules of Behavior annually. Information is shared in accordance with VA Handbook 6500. The principle of need-to-know is strictly adhered to by program office. Only personnel with a clear business purpose are allowed access to the system and the information contained within. This action adheres to the idea of least privilege and need to know found in the VA 6500 Handbook. Access to the system requires a VA issued identity assertion.

## **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*

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

*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:** Not applicable, as there is no sharing of information outside of VBA or VA with external parties. The SOAP Service purpose is to ingest documents into FFR.

**Mitigation:** Not applicable.

## 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 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?**

*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. If notice was provided in the Federal Register, provide the citation.*

*If notice was not provided, explain why. If it was provided, attach a copy of the current notice.*  
No notice is required or provided to individuals for consent to collect information for specific uses as no information is to be collected by the SOAP Service.

*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. This question is 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.*

Not applicable: No notice is provided to an individual. The SOAP Service does not collect information while ingesting documents into FFR.

**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*

Not applicable

**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*

Not applicable

**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.*

*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:** Not applicable

**Mitigation:** Not applicable

## 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?

*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.*

*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).*

*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. This question is related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.*

The SOAP Service does not allow individuals to gain access to their information as its primary function is to send information to FFR. Information is not collected.

### 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.*

Documents that are ingested by the SOAP Service have already been established. Inaccurate or erroneous information cannot be applied to these documents.

### 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 are not notified as the SOAP Service only ingests documents and cannot modify information contained in the ingested documents.

#### **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.*

*This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.*

*Example: Some projects allow users to directly access and correct/update their information online. This helps ensure data accuracy.*

Not applicable

#### **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.*

*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:** Not applicable

**Mitigation:** Not applicable

## 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?**

*Describe the process by which an individual receives access to the system.*

*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?*

*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.*

*This question is related to privacy control AR-7, Privacy-Enhanced System Design and Development.*

The SOAP application does not have user roles as its primary function is to ingest documents into the FTI File Repository. Only designated employees from the department of Veteran Affairs have access FTI SOAP. The designated employees have AWS Administrative access. FTI SOAP does not have a user interface.

### **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.*

Not applicable: Within the SOAP service VA contractors do not have access to FTI within FTI SOAP. Only designated employees from the department of Veteran Affairs have access FTI SOAP. The designated employees have AWS Administrative access. FTI SOAP does not have a user interface.

### **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.*

.FTI SOAP does not include a user interface and as such does not have end users. FTI SOAP interacts with legacy systems to store documents within the FTI Secure Enclave that are unable to conform to the REST interface provided by the FTI File Repository. Personnel that will be accessing information systems must read and acknowledge their receipt and acceptance of the VA National Rules of Behavior (ROB). The rules are included as part of the 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. All VA employees must complete annual Privacy and Security training. Users agree to comply with all terms and conditions of the National Rules of Behavior, by signing a certificate of training at the end of the training session.

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

*If Yes, provide:*

- 1. The Security Plan Status,*
- 2. The Security Plan Status Date,*
- 3. The Authorization Status,*
- 4. The Authorization Date,*
- 5. The Authorization Termination Date,*
- 6. The Risk Review Completion Date,*
- 7. The FIPS 199 classification of the system (LOW/MODERATE/HIGH).*

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

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

- 1. Security Plan Status: Approved*
- 2. Security Plan Status Date: December 18, 2020*
- 3. Authorization Status: Approved*
- 4. Authorization Date: January 21, 2021*
- 5. Authorization Termination Date: January 21, 2022*
- 6. Risk Review Completion Date: January 7, 2021*
- 7. FIPS 199 classification: High*

## 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).*

*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.*

The BIP Platform is deployed in a Federal Risk and Authorization Management Plan (FEDRAMP)-approved cloud service provider (CSP) environment. Security controls are managed at three levels: FEDRAMP, General Support Services (GSS), and the Platform level. FEDRAMP and GSS control details are available in VA Enterprise Cloud (VAEC) Amazon Web Services (AWS) accreditation documentation.

### 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)

*This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.*

<<ADD ANSWER HERE>>

### 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.*

<<ADD ANSWER HERE>>

**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.*

<<ADD ANSWER HERE>>

**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).*

<<ADD ANSWER HERE>>

Section 10. References

## Summary of Privacy Controls by Family

*Summary of Privacy Controls by Family*

<b>ID</b>	<b>Privacy Controls</b>
<b>AP</b>	<b>Authority and Purpose</b>
AP-1	Authority to Collect
AP-2	Purpose Specification
<b>AR</b>	<b>Accountability, Audit, and Risk Management</b>
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
<b>DI</b>	<b>Data Quality and Integrity</b>
DI-1	Data Quality
DI-2	Data Integrity and Data Integrity Board
<b>DM</b>	<b>Data Minimization and Retention</b>
DM-1	Minimization of Personally Identifiable Information
DM-2	Data Retention and Disposal
DM-3	Minimization of PII Used in Testing, Training, and Research
<b>IP</b>	<b>Individual Participation and Redress</b>
IP-1	Consent
IP-2	Individual Access
IP-3	Redress
IP-4	Complaint Management
<b>SE</b>	<b>Security</b>
SE-1	Inventory of Personally Identifiable Information
SE-2	Privacy Incident Response
<b>TR</b>	<b>Transparency</b>
TR-1	Privacy Notice
TR-2	System of Records Notices and Privacy Act Statements
TR-3	Dissemination of Privacy Program Information
<b>UL</b>	<b>Use Limitation</b>

<b>ID</b>	<b>Privacy Controls</b>
UL-1	Internal Use
UL-2	Information Sharing with Third Parties

**Signature of Responsible Officials**

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

---

**Privacy Officer, Simon Caines**

---

**Information Systems Security Officer, Joseph Guillory**

---

**System Owner, Gary Dameron**

## 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). .