Privacy Impact Assessment for the VA IT System called:

VHA Leadership & Workforce Development (VHALWD)

Workforce Solutions
VHA

Date PIA submitted for review:

Feb 3, 2022

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Socrates Gonzalez	socrates.gonzalez@va.gov	(405) 552-4348
Information System Security Officer (ISSO)	Steve Cosby	steve.cosby@va.gov	(919) 474-3928
Information System Owner	Chris Jaqua	Chris.jaqua@va.gov	(405) 552-4345

Abstract

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

The Veterans Health Administration (VHA) Leadership and Workforce Development System (VHALWD) contains information on people, positions, and organizations, work groups, workforce, workforce and leadership classes, workforce development programs and participation, personal development plans, supervisory levels, mentor and coach attributes, High Performance Development Model (HPDM) core competency, intern data, EEO reporting, succession planning, workforce planning, senior executive information, applicant tracking and recruitment, Executive Career Field (ECF) position and performance information, and education funding and programs. The method used to collect this information is a proprietary system using relational database technology. Information from these databases are joined and expanded to inform programs and processes. This combination of information is used in the administration of talent management, VHA human capital objectives, and in the support of the ERB and PRB functions.

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 Veterans Health Administration (VHA) Leadership and Workforce Development System (VHALWD) contains information on people, positions, and organizations, work groups, workforce, workforce and leadership classes, workforce development programs and participation, personal development plans, supervisory levels, mentor and coach attributes, High Performance Development Model (HPDM) core competency, intern data, EEO reporting, succession planning, workforce planning, senior executive information, applicant tracking and recruitment, Executive Career Field (ECF) position and performance information, and education funding and programs. The VHA Executive Management Program consists of the functions that fall under the purview of the VHA Executive Resources Board (ERB) and the VHA Performance Review Board (PRB). Their functions include executive development, recruitment and placement, organizational analysis, succession planning, workforce planning, EEO and ADR assessment, workload tracking and reporting of human capital and HR, and individual and organizational performance assessment and recognition. The method used to collect this information is a proprietary system using relational database technology. Information from these databases are joined and expanded to inform programs and processes. This combination of information is used in the administration of talent management, VHA human capital objectives, and in the support of the ERB and PRB functions. Information on approximately 350,000 VA employees is on the system. The HTM LAN and VHALWD major application are under Region 6. All information in the system is VA Employee related service information that is setup with internal sharing for VA Organizations and the OPM Federal Government Agency. The legal authorities are listed in any SORN that is associated with the system. Or either VA directive or congressional law.

Title 38, United States Code, Section 8127, Title 38, United States Code, Sections 501(a) and 501(b);, Title 38, United States Code, Sections 501(a), 1705, 1710, 1722, and 5317
161VA10A2 Veterans Health Administration Leadership and Workforce Development-Title 38, United States Code, section 501a https://www.gpo.gov/fdsys/pkg/FR-2010-02-22/pdf/2010-3298.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://vaww.va.gov/vapubs/). If the system creates information (for example, a score, analysis, or report), list the information the system is responsible for creating.

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

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

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

- ☒ Name
- ☒ Social Security Number
- ☒ Date of Birth
- ☒ Mother's Maiden Name
- ☒ Personal Mailing Address
- ☒ Personal Phone Number(s)
- ☒ Personal Fax Number
- ☒ Personal Email Address
- ☒ Emergency Contact Information (Name, Phone Number, etc. of a different individual)
- ☒ Financial Account Information
- ☐ Health Insurance Beneficiary Numbers Account numbers
- ☐ Certificate/License numbers
- ☐ Vehicle License Plate Number
- ☐ Internet Protocol (IP) Address Numbers
- ☐ Current Medications
- ☐ Previous Medical Records
- ☒ Race/Ethnicity
- ☐ Tax Identification Number
- ☐ Medical Record Number
- ☒ Gender
- ☐ Integration Control Number (ICN)
- ☐ Military History/Service Connection
- ☐ Next of Kin
- ☒ Other Unique Identifying Information (list below)
  - *Grade
  - *SF52
  - * Disability
  - * National Origin

PII Mapping of Components

VHALWD consists of 49 key components (databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by **VHALWD** 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
Data.htm.va.gova ARPA aspRoleManagement CDW DataFeeds Education_Documentation EEODemographics EMI ExternalCustomers HLTIBudget HLTITalentManagement HPDM_Documents HR_Administration HR_Classification HR_Staffing hrro_education HRSmart HTM HTM_Documents IndividualAssessment PAID PCMM ProgramEvaluation RecurringReports USAStaffing VacancyTracking VHALWD Wmctravel WorkforcePlanning Working	**YES**	**YES**	SSN, DoB, Full name, Home Address, email address	Utilized by WebHR software app in support of HR activities	Authentication/Authorization controls with access limited to assigned Roles to approved users. Access removed when users leave or change positions. Use of Delta tables to monitor changes. Information is masked on screen for authorized users, not displayed for all others

Data.htm.va.gov aes dbaTools distribution ErrorHandling HelpDesk_WRRS HPDM_Messaging HR_Global HR_Processing HR_Reports Master Model Msdb PAID_Reports ReportServer ReportServerTempDB SystemState Tempdb VA_Organizations Vacancies Vulcan	NO	NO			

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.

Received via electronic transmission from PAID, Active Directory, Nature of Action, Employee and Payroll, HRSmart.

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.

Received via electronic transmission from PAID, Active Directory, Nature of Action, Employee and Payroll, HRSmart.

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.

Data is received and checked daily and weekly from our data sources upstream. Active Directory, Nature of Action, Employee and Payroll, HRSmart. These systems are responsible for checking the accuracy and their processes can be found in their PIA. Our databases go above requirements and also does basic system checks to verify the integrity of the database.

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 legal authorities are listed in any SORN that is associated with the system. Or either VA directive or congressional law.

Title 38, United States Code, Section 8127, Title 38, United States Code, Sections 501(a) and 501(b);, Title 38, United States Code, Sections 501(a), 1705, 1710, 1722, and 5317

161VA10A2 Veterans Health Administration Leadership and Workforce Development-Title 38, United States Code, section 501a https://www.gpo.gov/fdsys/pkg/FR-2010-02-22/pdf/2010-3298.pdf

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

Consider the specific data elements collected and discuss the potential privacy risks and what steps, if any are currently being taken to mitigate those identified risks.

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: Due to the sensitive nature of this data, there is a risk that, if the data were accessed or received by unauthorized parties/recipients or otherwise breached, serious personal, professional and/or financial harm may result for the affected individuals. VA would be required to provide credit monitoring and ID theft insurance.

Mitigation: VHALWD uses a number of security measures designed to ensure that the information is not inappropriately disclosed or released. Use of encryption to secure data during transmission and at rest; user information security and privacy education and training; restricted use of removable media, weekly administrative rounds to identify any potential issues, security screens and secure mailing. The measures also include, access controls, security assessments, contingency planning; incident response, system and communications protection. Our facility employs all security controls in the respective high impact control baseline unless specific exceptions have been allowed based on

the guidance provided in the National Institute of Standards and Technology (NIST) Special Publication 800-37 and specific VA directives.

The VHALWD applications are built using VA active directory roles and permissions. The VHALWD helpdesk has the process documented and assists users throughout VA. Security baselines approved by VA are in place on each SQL server to add additional protection.

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.

- Used to identify the VA employee for reports and VA application functions such as HR management in WebHR.
    - **Name:** Used to identify the VA employee for reports and VA application functions such as HR management in WebHR.
    - **Social Security Number:**
    - **Date of Birth:**
- Used for reports and VA application functions such as HR management in WebHR.
    - **Mother's Maiden Name:**
    - **Personal Mailing Address:**
    - **Personal Phone Number:**
    - **Personal Fax Number:**
    - **Personal Email Address:**
    - **Emergency Contact:**
    - **Race/Ethnicity:**
    - **Grade:**
    - **SF52:**
    - **Gender:**
    - **Disability:**

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

Tools used are VA's licensed ProClarity and pyramid analytics software. Pyramid is replacing ProClarity as VA's standard analytics software. A recent example report would be the VA Secretary and team asking how many VA vacant positions have been filled. Data is used to produce valuable reports for national leadership and succession planning, members of congress, FOIA and other data calls in addition to the HR and other web applications mentioned above.

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

All SSNs are in SQL databases. All SQL databases have Transparent Data Encryption (TDE) applied. As a common practice, we do scramble our SSN fields in our non-production applications. Our approach is not to show the SSN in our applications unless there is an absolute need. In those cases, we will display the last 4. In our production databases, the data we get for PAID and HRSmart has the full SSN. We also use role-based restrictions for both database and applications. We follow the principle of least privilege.

2.4 <u>PRIVACY IMPACT ASSESSMENT: Use of the information.</u> 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. <u>Example: Describe if training for users of the project</u>

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.

Add answer here:

The baseline security requirements and safeguards cover a large number of security-related areas with regard to protecting the confidentiality, integrity, and availability of VA information systems and the information processed, stored, and transmitted by those systems. The security-related areas include: access control; awareness and training; audit and accountability; certification, accreditation, and security assessments; configuration management; contingency planning; identification and authentication; incident response; maintenance; media protection; physical and environmental protection; planning; personnel security; risk assessment; systems and services acquisition; system and communications protection; and system and information integrity. Our facility employs all security controls in the respective impact security control baseline unless specific exceptions have been allowed based on the tailoring guidance provided in NIST Special Publication 800-53 and specific VA directives. An updated PIA, PTA and SORN are all in place and updated on the VA approved schedule.

The application is role specific and requires approval to receive roles to access information through active directory. Safeguards include a VA baselined SQL database, servers and VA Cybersecurity Operations Center recurring scans such as PIN testing for servers, WASA scans for applications and database scans. Users complete recurring training in handling PII to include the yearly VA rules of behavior training and more detailed WS helpdesk standard operating procedures. The WS helpdesk manages access to roles and if requested by supervisors can remove access for disciplinary reasons.

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:
Mailing Address:
Zip Code:
Phone Number:
Fax Number:
Email Address:
Emergency Contact:
Race:
Grade:
SF52:
Gender:
Disability:

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. 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.

Documents are required for retention following the guidance in Guide to Personnel Recordkeeping (GPR) which clearly outlines documents required for long term retention and/or transfer. The Title V of the Code of Federal Regulations (CFR), § 293.405 which explains the retention period for SES and non-SES performance rating of record. Finally, the eOPF Master Forms List identifies forms designated as Permanent, Temporary, and Agency specific documents for both Title V and non-Title V organizations for those agencies that have migrated to eOPF. The retention period is dependent on the type of data and the intended use. VA Records Control Schedule 10-1 (page 8) has Records Management Responsibilities for developing policies and procedures for effective and efficient records management throughout VHA. Program officials are responsible for creating, maintaining, protecting, and disposing of records in their program area in accordance with National Archives and Records Administration (NARA) regulations and VA policy. All VHA employees are responsible to ensure that records are created, maintained, protected, and disposed of in accordance with NARA regulations and VA policies and procedures.

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.

Yes, documents are required for retention following the guidance in Guide to Personnel Recordkeeping (GPR) which clearly outlines documents required for long term retention and/or transfer. The Title V of the Code of Federal Regulations (CFR), § 293.405 which explains the retention period for SES and non-SES performance rating of record. Finally, the eOPF Master Forms List identifies forms designated as Permanent, Temporary, and Agency specific documents for both Title V and non-Title V organizations for those agencies that have migrated to eOPF. The retention period is dependent on the type of data and the intended use. VA Records Control Schedule 10-1 (page 8) has Records Management Responsibilities for developing policies and procedures for effective and efficient records management throughout VHA. Program officials are responsible for creating, maintaining, protecting, and disposing of records in their program area in accordance with National Archives and Records Administration (NARA) regulations and VA policy. All VHA employees are responsible to ensure that records are created, maintained, protected, and disposed of in accordance with NARA regulations and VA policies and procedures.

RCS 10-1 link for VHA: www.va.gov/vhapublications/rcs10/rcs10-1.pdf
RCS VB-1, Part II Revised for VBA:
www.benefits.va.gov/WARMS/docs/admin20/rcs/part2/part2.pdf

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

Applicable federal regulatory requirements (NARA & VHA Records Control Schedule 10-1) will be followed for eliminating or disposing of data. We electronically retrieve our data from other sources as described above. Our upstream resources eliminate records based on the records control schedules and we download the refreshed data. Paper records that are able to be shredded are done so onsite by a certified shredding company. Old hard drives from computers are destroyed as well with a certificate of destruction. For the database, the upstream data sources remove records as required by their retention period and policy and that data is received by our downstream database.

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

For the development and training environments, PII such as an SSN is scrambled to protect the data.

The baseline security requirements and safeguards cover a large number of security-related areas with regard to protecting the confidentiality, integrity, and availability of VA information systems and the information processed, stored, and transmitted by those systems. The security-related areas include: access control; awareness and training; audit and accountability; certification, accreditation, and security assessments; configuration management; contingency planning; identification and authentication; incident response; maintenance; media protection; physical and environmental protection; planning; personnel security; risk assessment; systems and services acquisition; system and communications protection; and system and information integrity. Our facility employs all security controls in the respective impact security control baseline unless specific exceptions have been allowed based on the tailoring guidance provided in NIST Special Publication 800-53 and specific VA directives. An updated PIA, PTA and SORN are all in place and updated on the VA approved schedule.

The application is role specific and requires approval to receive roles to access information through active directory. Safeguards include a VA baselined SQL database, servers and VA Cybersecurity Operations Center recurring scans such as PIN testing for servers, WASA scans for applications and database scans. Users complete recurring training in handling PII to include the yearly VA rules of behavior training and more detailed WS helpdesk standard operating procedures. The WS helpdesk manages access to roles and if requested by supervisors can remove access for disciplinary reasons.

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

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

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: The baseline security requirements and safeguards cover a large number of security-related areas with regard to protecting the confidentiality, integrity, and availability of VA information systems and the information processed, stored, and transmitted by those systems. The security-related areas include: access control; awareness and training; audit and accountability; certification, accreditation, and security assessments; configuration management; contingency planning; identification and authentication; incident response; maintenance; media protection; physical and environmental protection; planning; personnel security; risk assessment; systems and services acquisition; system and communications protection; and system and information integrity. Our facility employs all security controls in the respective impact security control baseline unless specific exceptions have been allowed based on the tailoring guidance provided in NIST Special Publication 800-53 and specific VA directives. An updated PIA, PTA and SORN are all in place and updated on the VA approved schedule.

Mitigation: The application is role specific and requires approval to receive roles to access information through active directory. Safeguards include a VA baselined SQL database, servers and VA Cybersecurity Operations Center recurring scans such as PIN testing for servers, WASA scans for applications and database scans. Users complete recurring training in handling PII to include the yearly VA rules of behavior training and more detailed WS helpdesk standard operating procedures. The WS helpdesk manages access to roles and if requested by supervisors can remove access for disciplinary reasons.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

4.1 With which internal organizations is information shared/received/transmitted? What information is shared/received/transmitted, and for what purpose? How is the information transmitted?

NOTE: Question 3.9 (second table) on Privacy Threshold Analysis should be used to answer this question.

Identify and list the names of any program offices, contractor-supported IT systems, and any other organization or IT system within VA with which information is shared.

State the purpose for the internal sharing. If you have specific authority to share the information, provide a citation to the authority.

For each interface with a system outside your program office, state what specific data elements (PII/PHI) are shared with the specific program office, contractor-supported IT system, and any other organization or IT system within VA.

Describe how the information is transmitted. For example, is the information transmitted electronically, by paper, or by some other means? Is the information shared in bulk, on a case-by-case basis, or does the sharing partner have direct access to the information?
This question is related to privacy controls AP-2, Purpose Specification, AR-3, Privacy Requirements for Contractors and Service Providers, AR-8, Accounting of Disclosures, TR-1, Privacy Notice, and UL-1, Internal Use.

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system***	***Describe the method of transmittal***
PAID	Received from VA source for VA Internal reports, data calls, FOIA requests and VHALWD web applications data for employees	Full name, social security number, date of birth, race national origin, handicap status, and performance rating, VHA, VBA, and NCA	SFTP
Active Directory	Received from VA source for VA Internal reports, data calls, FOIA requests and VHALWD web applications data for employees	Received from VA source for Database items from section 2 above Used for reports and VA application functions such as HR management in the WebHR application.	Electronic/File Transfer

List the Program Office or IT System information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT system*	*List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system*	*Describe the method of transmittal*
Nature of Action	Received from VA source for VA Internal reports, data calls, FOIA requests and VHALWD web applications data for employees	Full name, social security number, date of birth, race national origin, handicap status, and performance rating	Electronic/File Transfer/SFTP
Employee and Payroll	Received from VA source for VA Internal reports, data calls, FOIA requests and VHALWD web applications data for employees	Full name, social security number, date of birth	Electronic/File transfer
HRSmart	Received from VA source for VA Internal reports, data calls, FOIA requests and VHALWD web applications data for employees	Full name, social security number, Address, email, date of birth, race national origin, handicap status, and performance rating, VHA, VBA, and NCA	SFTP

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

Discuss the privacy risks associated with the sharing of information within the Department and what steps, if any, are currently being taken to mitigate those identified risks.
This question is related to privacy control UL-1, Internal Use.

Follow the format below:

Privacy Risk: Due to the sensitive nature of this data, there is a risk that, if the data were accessed or received by unauthorized parties/recipients or otherwise breached, serious personal, professional and/or financial harm may result for the affected individuals. VA would be required to provide credit monitoring and ID theft insurance.

Mitigation: Procedures will be enforced using technical and managerial control mechanisms including following the Records Control Schedule (RCS) 10-1 VA guidance and having a disposal authority and log files for past and future suspense notices. The baseline security requirements and safeguards cover a large number of security-related areas with regard to protecting the confidentiality, integrity, and availability of VA information systems and the information processed, stored, and transmitted by those systems. The security-related areas include: access control; awareness and training; audit and accountability; certification, accreditation, and security assessments; configuration management; contingency planning; identification and authentication; incident response; maintenance; media protection; physical and environmental protection; planning; personnel security; risk assessment; systems and services acquisition; system and communications protection; and system and information integrity. Our facility employs all security controls in the respective impact security control baseline unless specific exceptions have been allowed based on the tailoring guidance provided in NIST Special Publication 800-53 and specific VA directives. An updated PIA, PTA and SORN are all in place and updated on the VA approved schedule.

The application is role specific and requires approval to receive roles to access information through active directory. Safeguards include a VA baselined SQL database, servers and VA Cybersecurity Operations Center recurring scans such as PIN testing for servers, WASA scans for applications and database scans. Users complete recurring training in handling PII to include the yearly VA rules of behavior training and more detailed WS helpdesk standard operating procedures. The WS helpdesk manages access to roles and if requested by supervisors can remove access for disciplinary reasons

Section 5. External Sharing/Receiving and Disclosure

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

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

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

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

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

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

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

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

Data Shared with External Organizations

List External Program Office or IT System information is shared/received with	***List the purpose of information being shared / received / transmitted with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted)with the Program or IT system***	***List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)***	***List the method of transmission and the measures in place to secure data***
eOPF	Extracts from the VHALWD to the OPM system	Database items including VA employee name, SSN and performance appraisal documents to be loaded into eOPF.	MOU/ISA/ICD	Electronic/File Transfer/IBM Connect Direct
USAStaffing	Retrieves OPM	Name, Financial Information	MOU/ISA/ICD	SFTP
Salesforce	Retrieves HR data from Salesforce	Full name, target grade, hiring related data fields	MOU/ISA/ICD	SFTP/DSS

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: Due to the sensitive nature of this data, there is a risk that, if the data were accessed or received by unauthorized parties/recipients or otherwise breached, serious personal, professional and/or financial harm may result for the affected individuals. VA would be required to provide credit monitoring and ID theft insurance.

Mitigation: Procedures will be enforced using technical and managerial control mechanisms including following the Records Control Schedule (RCS) 10-1 VA guidance and having a disposal authority and log files for past and future suspense notices. The baseline security requirements and safeguards cover a large number of security-related areas with regard to protecting the confidentiality, integrity, and availability of VA information systems and the information processed, stored, and transmitted by those systems. The security-related areas include: access control; awareness and training; audit and accountability; certification, accreditation, and security assessments; configuration management; contingency planning; identification and authentication; incident response; maintenance; media protection; physical and environmental protection; planning; personnel security; risk assessment; systems and services acquisition; system and communications protection; and system and information integrity. Our facility employs all security controls in the respective impact security control baseline unless specific exceptions have been allowed based on the tailoring guidance provided in NIST Special Publication 800-53 and specific VA directives. An updated PIA, PTA and SORN are all in place and updated on the VA approved schedule.

The application is role specific and requires approval to receive roles to access information through active directory. Safeguards include a VA baselined SQL database, servers and VA Cybersecurity Operations Center recurring scans such as PIN testing for servers, WASA scans for applications and database scans. Users complete recurring training in handling PII to include the yearly VA rules of behavior training and more detailed WS helpdesk standard operating procedures. The WS helpdesk manages access to roles and if requested by supervisors can remove access for disciplinary reasons.

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.

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.

Multiple notices below and a system of records notice 161VA10A2
Federal Register :: Privacy Act of 1974; System of Records
2018-05087.pdf (govinfo.gov)

Initial Warning/Acknowledgement, and when user session expires:

"This U.S. Government computer system contains sensitive information and is for official use only. Any information exported from this application to your desktop, requires the same level of security as appropriate action on any information of a sensitive nature.

Activity on this system is monitored. Use of this system constitutes your unconditional consent to such monitoring and no expectation of privacy. Misuse of, unauthorized access to, or attempted unauthorized access to this system will result in administrative disciplinary action and/or criminal prosecution as appropriate."

Button to click : "I Acknowledge"

Session Time out Warning:

"Session is Expiring!" Occurs when 20 minutes of inactivity.

"Session (Page) Expired!" Occurs when 20 minutes 30 seconds of no activity.

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

Certain information is required by VA HR when being hired. Information is VA employment and demographic data. The VA employee has the right to work with his or her HR office on what information they provide.

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

Certain information is required by VA HR when being hired. Information is VA employment and demographic data. The VA employee has the right to work with his or her HR office on what information they provide.

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.

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

<u>Principle of Transparency:</u> Has sufficient notice been provided to the individual?

<u>Principle of Use Limitation:</u> 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: The risk for not providing notice would be a lack of transparency and the employee not being aware of the system's use of information.

Mitigation: Procedures will be enforced using technical and managerial control mechanisms including following the Records Control Schedule (RCS) 10-1 VA guidance and having a disposal authority and log files for past and future suspense notices. The baseline security requirements and safeguards cover a large number of security-related areas with regard to protecting the confidentiality, integrity, and availability of VA information systems and the information processed, stored, and transmitted by those systems. The security-related areas include: access control; awareness and training; audit and accountability; certification, accreditation, and security assessments; configuration management; contingency planning; identification and authentication; incident response; maintenance; media protection; physical and environmental protection; planning; personnel security; risk assessment; systems and services acquisition; system and communications protection; and system and information integrity. Our facility employs all security controls in the respective impact security control baseline unless specific exceptions have been allowed based on the tailoring guidance provided in NIST Special Publication 800-53 and specific VA directives. An updated PIA, PTA and SORN are all in place and updated on the VA approved schedule.

The application is role specific and requires approval to receive roles to access information through active directory. Safeguards include a VA baselined SQL database, servers and VA Cybersecurity Operations Center recurring scans such as PIN testing for servers, WASA scans for applications and database scans. Users complete recurring training in handling PII to include the yearly VA rules of behavior training and more detailed HCSS helpdesk standard operating procedures. The WMC helpdesk manages access to roles and if requested by supervisors can remove access for disciplinary reasons.

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.

Employees update their data through HRSmart and PAID systems. Employees can also access https://htm2.va.gov/ for HTM applications. Employees work with their HR office for procedures for updating their information. Employees can access HRSmart at https://ssologon.iam.va.gov/CentralLogin/ and MyPay at https://mypay.dfas.mil/mypay.aspx.

To request a FOIA request outside of VA, see instructions at http://www.foia.gov/how-to.html

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.

Employees update their data through HRSmart and PAID systems. Employees can also access https://htm2.va.gov for HTM applications. Employees work with their HR office for procedures for updating their information. Employees can access HRSmart at https://ssologon.iam.va.gov/CentralLogin/ and MyPay at https://mypay.dfas.mil/mypay.aspx.

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.

Employees update their data through HRSmart and PAID systems. Employees can also access https://htm2.va.gov for HTM applications. Employees work with their HR office for procedures for updating their information. Employees can access HRSmart at https://ssologon.iam.va.gov/CentralLogin/ and MyPay at https://mypay.dfas.mil/mypay.aspx.

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 ensures data accuracy.

Employees update their data through HRSmart and PAID systems. Employees can also access https://htm2.va.gov for HTM applications. Employees work with their HR office for procedures for updating their information. Employees can access HRSmart at https://ssologon.iam.va.gov/CentralLogin/ and MyPay at https://mypay.dfas.mil/mypay.aspx.

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: **N/A – VA employees can update their employee information whenever they need to.**

Mitigation: Employees update their data through HRSmart and PAID systems. Employees can also access https://htm2.va.gov/ for HTM applications. Employees work with their HR office for procedures for updating their information. Employees can access HRSmart at https://ssologon.iam.va.gov/CentralLogin/ and MyPay at https://mypay.dfas.mil/mypay.aspx.

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 VHALWD applications are built using VA active directory roles and permissions. The WS helpdesk has the process documented and assists users throughout VA. Security triggers approved by VA NSOC are in place on each SQL server to add additional protection.

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.

Yes, the WS helpdesk has multiple contractors working to assist VA employees. The contractors are not involved in design and maintenance. Contracts are reviewed yearly by WS staff and the contracting officer. Background checks and clearance have been obtained prior to contractors starting work.

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.

Yearly training is required for all users including additional training for managing PII and paperwork for PII including VA Privacy and information security awareness and rules of behavior and Annual Government Ethics Training. Additional training and standard operating procedures are managed at the team helpdesk level.

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.***

Yes.

1. The Security Plan Status: Approved
2. The Security Plan Status Date: 01-Mar-2021
3. The Authorization Status - Authorization to Operate (ATO)

4. The Authorization Date: 28-April-2021
5. The Authorization Termination Date: 20-Apr-2024
6. The Risk Review Completion Date: 7-Apr-2021
7. The FIPS 199 classification of the system (LOW).

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.

VHALWD does not use Cloud Technology.

9.2 Does the contract with the Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII? (Provide contract number and supporting information about PII/PHI from the contract)

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

N/A. VHALWD does not utilize cloud services.

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

Per NIST 800-144, cloud providers hold significant details about the accounts of cloud consumers that could be compromised and used in subsequent attacks. Ancillary data also

involves information the cloud provider collects or produces about customer-related activity in the cloud. It includes data collected to meter and charge for consumption of resources, logs and audit trails, and other such metadata that is generated and accumulated within the cloud environment.

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

N/A. VHALWD does not utilize cloud services.

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

What are the roles and responsibilities involved between the organization and cloud provider, particularly with respect to managing risks and ensuring organizational requirements are met?

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

N/A. VHALWD does not utilize cloud services.

9.5 If the system is utilizing Robotics Process Automation (RPA), please describe the role of the bots.

Robotic Process Automation is the use of software scripts to perform tasks as an automated process that executes in parallel with or in place of human input. For example, will the automation move or touch PII/PHI information. RPA may also be referred to as "Bots" or Artificial Intelligence (AI).

N/A

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**

ID	Privacy Controls
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.

Socrates N. Gonzalez 255689

Digitally signed by Socrates N. Gonzalez 255689
Date: 2022.03.17 09:09:16 -05'00'

Privacy Officer, Socrates Gonzalez

Steve M. Cosby 223809

Digitally signed by Steve M. Cosby 223809
Date: 2022.03.17 08:05:57 -04'00'

Information System Security Officer, Steve Cosby

Christopher A. Jaqua 230743

Digitally signed by Christopher A. Jaqua 230743
Date: 2022.03.17 07:41:33 -05'00'

Information System Owner, Chris Jaqua

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).