Privacy Impact Assessment for the VA IT System called:

Human Resources Information Systems

(HR Smart)

Veterans Health Administration (VHA)

Center for Enterprise Human Resources Information Services (CEHRIS)

Date PIA submitted for review:

06/22/2023

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Nevalan Orr	Nevalan.Orr@va.gov	202-461-1524

	Name	E-mail	Phone Number
Information System Security Officer (ISSO)	La Toya Butler-Cleveland	LaToya.Butler-Cleveland@va.gov	(202) 503-7542
Information System Owner	Ricardo Osborne	Ricardo.Osborne@va.gov	202-360-6964

Abstract

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

The Human Resources Information System (HRIS, HR Smart), also known as HR Smart, is a Department of Veterans Affairs (VA) Human Capital Management information system that provides integrated personnel action and benefits processing for more than 320,000 VA employees and 100,000 clinical trainees.

Overview

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

1 General Description

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

The HR Smart system is a Department of Veterans Affairs (VA) Center for Enterprise Human Resources Information Services (CEHRIS).

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

HR Smart is considered a major application and serves as the enterprise's central human resources system for all of VA's 320,000 employees and 100,000 clinical trainees. HR Smart is built on PeopleSoft Enterprise Human Resources, an Oracle-owned, commercial off-the-shelf (COTS) product. HR Smart provides tools for the VA to better manage its workforce and provide enhancements such as self-service options for VA managers and employees. HR Smart provides VA with core functions for processing personnel actions, benefits management, and compensation management. HR Smart collects, maintains, stores, and shares PII and SPI of these associated users of the system. To execute these core functions, HR Smart will maintain personnel and HR data for the VA workforce, including names, social security numbers, contact information, compensation data, and benefits information. The verification of appropriate users allows the system to ensure there is no unauthorized access to view human resource data for VA.

HR Smart has enhanced its system by incorporating TXP to unify the experience layer, allowing VA to modernize and begin gaining the benefits of a better employee experience. TXP offers users of the HR Smart system an enhanced and integrated user interface, workflows, and reporting capabilities. TXP is an IBM software as a system (SaaS) solution built with ServiceNow HR Service Delivery.

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

IBM provides operations and maintenance support for HR Smart. The PeopleSoft module of HR Smart is hosted in the QTS hosting facility, with a primary site in Dulles, Virginia, and alternate site in Phoenix, Arizona. The Talent Experience Platform (TXP) module of HR Smart leverages the software as a service, FedRAMP certified, ServiceNow system, located in Culpepper, Virginia, and Miami, Florida.

2. Information Collection and Sharing

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

HR Smart serves as the enterprise's central human resources system for all of VA's 320,000 employees and 100,000 clinical trainees. These users are primarily located VA-wide. HR Smart allows VA to better manage its workforce and will provide enhancements such as self-service options for VA managers and employees.

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

HR Smart provides tools for the VA to better manage its workforce and provide enhancements such as self-service options for VA managers and employees. information.

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

To provide tools for the VA to better manage its workforce and provide enhancements, the HR Smart system has interconnections with other applications and information systems listed in section 4 below. HR Smart provides VA with core functions for processing personnel actions, benefits management, and compensation management. HR Smart collects, maintains, stores, and shares PII and SPI of these associated users of the system. To execute these core functions, HR Smart will maintain personnel and HR data for the VA workforce, including names, social security numbers, contact information, compensation data, and benefits

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

The HR Smart team has implemented required security and privacy controls for Federal information systems and organizations according to NIST SP 800-53 and VA Handbook 6500, Risk Management Framework for VA Information Systems. Per the approval of the authorizing official, HR Smart maintains an Authority to Operate (ATO) at the Federal Information Security Management Act (FISMA) Moderate categorization.

3. Legal Authority and SORN

H. *A citation of the legal authority to operate the IT system.*
- *Title 38, United States Code, Sections 501(a), 1705, 1710, 1722, and 5317*
- *Information from SORN 171VA056A: 38 U.S.C. 501(a); 38 U.S.C. 73; 38 U.S.C. 75 SEC 4202; 5 U.S.C. Part III, Subparts D and E*
- *5 U.S.C. 552, "Freedom of Information Act," c. 1967*
- *5 U.S.C. 552a, "Privacy Act," c. 1974*
- *OMB Circular A-130, Appendix III, "Security of Federal Automated Information Systems"*
- *Information Technology Management Reform Act of 1996 (also known as the Clinger-Cohen Act)*
- *Federal Information Security Management Act (FISMA) of 2002*
- *OMB M-03-22, "OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*
- *VA Directive and Handbook 6502, Privacy Program*

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

The HR Smart system is not in the process of being modified.

D. System Changes

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

The completion of this PIA will not result in circumstances that require changes to the business process.

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

The completion of this PIA will not result in technology changes.

Section 1. Characterization of the Information

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

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

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

If a requesting system receives information from another system, such as a response to a background check, describe what information is returned to the requesting system.

This question is related to privacy control AP-1, Authority To Collect, and AP-2, Purpose Specification.

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

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

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

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

HR Smart contains VA position and employee data, such as compensation data and benefits information. Information includes payroll, VA accounting, pay and leave entitlement records, payroll deduction and withholding, and time and attendance. Name and compensation information is subject to disclosure under the Freedom of Information Act and is routinely provided by the Office of Personnel Management to the media on request. Additional information includes employee social security numbers, and voluntarily self-reported race, national origin, and ethnicity data. Such data are considered to be Personally Identifiable Information (PII) and are the most sensitive information elements included in the system. Other information includes payroll, VA accounting, pay and leave entitlement records, payroll deduction and withholding, and time and attendance. However, no Personal Health Information (PHI) is collected, used, maintained and/or shared. The PII and SPI data that is collected allows HR Smart to function at its full capability. The addition of the TXP module does not precipitate or impact the collection, storage, or transfer of SSNs as established in the system.

PII Mapping of Components (Servers/Database)

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

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

Internal Database Connections

Database Name of the information system collecting/storing PII	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
HR Smart PeopleSoft Database (Oracle PeopleSoft Human Capital Management)	Yes	Yes	Name Social Security Number Date of Birth Personal Mailing Address Personal Phone Number(s) Personal Email Address Emergency Contact Information Financial Account Information Health Insurance Beneficiary Numbers Race/Ethnicity Gender Military History/Service Connection Next of Kin VA Employee and Compensation Data	Human Resources and benefits distribution	For all sensitive data / PII, cryptographic protections are used for both data at rest and data in transit (external and internal). HR Smart employs FIPS 140-2 validated encryption modules and supports FIPS 140 2 validated encryption mechanisms. • Encryption of data at rest for all HR Smart operational environments is provided by the Pure storage array which is FIPS 140-2 certified and validated. All HR Smart backups are encrypted by Veritas NetBackup which is also FIPS 140-2 certified and validated. • Encryption

					of Information in transit between the customer and HR Smart is provided by an IPSec site-to-site VPN Tunnel over the Equinox Exchange fabric. The IPSec site to site VPN tunnel utilizes AES256 encryption and SHA1 authentication algorithm, which is a FIPS140-2 compliant encryption mechanism. • Also, all information sent between the HR Smart Application tiers is encrypted and protected by the use of TLS 1.2 encryption, SSL certificates, machine keys, and software license keys.
HR Smart TXP Instance (ServiceNow)	Yes	Yes	Name Personal Mailing Address Personal Phone Number(s) Personal Email Address Race/Ethnicity VA Position and Compensation Data	Human resources user interface	For all sensitive data / PII, cryptographic protections are used for both data at rest and data in transit (external and internal). HR Smart employs FIPS 140-2 validated encryption modules and supports FIPS 140 2 validated encryption mechanisms. • Encryption of Information in

					transit between the customer and HR Smart is provided by an IPSec site-to-site VPN Tunnel over the Equinox Exchange fabric. The IPSec site to site VPN tunnel utilizes AES256 encryption and SHA1 authentication algorithm, which is a FIPS140-2 compliant encryption mechanism. • Also, all information sent between the HR Smart Application tiers is encrypted and protected by the use of TLS 1.2 encryption, SSL certificates, machine keys, and software license keys.

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

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

HR Smart is interconnected with several HR systems within the VA and other Federal agencies. Information is provided to HR Smart through system interfaces internal and external to the VA. Systems currently interfacing with HR Smart include: VA Time and Attendance System (VATAS); VA Office of Inspector General (OIG); VA Learning University Education Data Repository (VALU EDR); VA Hospital Administration Leadership & Workforce Development System (VHA LWD); VA Identify and Access Management Service (IAM); DFAS Defense Civilian Pay System (DCPS); electronic Official Personnel Folder (eOPF); Electronic Human Resources Integration (EHRI); DFAS myPay Web Application (myPay); DFAS myPay Master PIN Database (MPDB); Intelligent Automation Platform (IAP); Federal Employee Health benefits [FEHB] Data Hub; Monster Government Solutions (MGS)MHME (eClass360)

1.2b Describe why information from sources other than the individual is required. For example, if a program's system is using data from a commercial aggregator of information or data taken from public Web sites, state the fact that this is where the information is coming from and then in question indicate why the system is using this source of data.

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

Internal Interfaces:

- VA Time and Attendance System (VATAS): VATAS is an application that processes VA employee data, comprised of additions, changes, and separations of VA employees.
- VA Office of Inspector General (OIG): The OIG Netezza system is a data repository that supports custom reporting capabilities required by the VA's Office of Inspector General for the purpose of conducting audits, research and related activities.
- VA Learning University Education Data Repository (VALU EDR): EDR is an internal VA database that serves as the primary data source for VA Talent Management System (TMS) user profiles, maintaining strategic personnel demographic data to support TMS Operations.
- VA Hospital Administration Leadership & Workforce Development System (VHA LWD): The VHALWD system provides information on people, work groups, workforce, funding, leadership development, workforce development, personal development plans, supervisory levels and reporting relationships, mentor and coach relationships and certification, HTM core competencies, senior executive information and recruitment, human resources automation, position management, organization management, Executive Career Field information, and locations of VHA top management positions.

External Interfaces:

- OPM electronic Official Personnel Folder (eOPF): In compliance with the mission of the EHRI initiative to improve the Federal Government's human capital management through electronic access, eOPF serves as the electronic Official Personnel File, which is accessible by other Partner Agencies.
- OPM Electronic Human Resources Integration (EHRI): EHRI systems establish a data repository to accept Federal HR data that will act as a hub for data exchanges between Agencies and provide a hosting environment to be used by Agencies for an electronic Official Personnel Folder.
- OPM (USAStaffing): USA Staffing is an on-line recruitment and applicant management system that facilitates screening and hiring of new employees. The system is accessible via an Internet capable web browser. Applicant and certificate data are processed and stored. Data may also be transmitted electronically through a web services interface with an agency system.
- DFAS Defense Civilian Pay System (DCPS): DCPS is the standard Department of Defense civilian pay system. DFAS uses DCPS to standardize civilian payroll policies, processes, systems, and procedures throughout the Department, paying approximately 1,000,000 employees.
- DFAS myPay Web Application (myPay): The myPay Web Application is a system that allows Federal employees to view and make changes to their payroll and associated personnel records. These changes can be performed through an internet capable web browser and are then forwarded to the appropriate interfacing pay system for processing through the normal payroll process.
- DFAS myPay Master PIN Database (MPDB): The myPay MPDB provides the authentication mechanism for the myPay Web Application. Stored in myPay MPDB are each myPay user's personal credentials to include name, SSN, user ID, email address, service affiliation, and limited account access historical information.
- Intelligent Automation Platform (IAP) is a comprehensive automation solution which utilized unattended RPA to perform initial triage and handling of mail associated with Veterans benefits. This application processes scanned documents and additional functions that are performed include automated capture of data, Quality assurance (QA) of data and images as well as reporting on each of those components in a comprehensive Business Intelligence (BI) platform.
- Federal Employee Health benefits [FEHB] Data Hub facilitates electronic submission of employee Health Benefit enrollment information. Federal Agencies electronically transmit Federal Employees Health Benefits 2809/2810 enrollment data to OPM-Macon.
- Monster Government Solutions (MGS)MHME (eClass360) is a Position Classification System that allows the VA to create position descriptions and functional statement and associated documentation. It allows for the creation, storage and routing of these documents for the appropriate business process flow.

1.3 How is the information collected?

These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

1.3a This question is directed at the means of collection from the sources listed in question 1.2. Information may be collected directly from an individual, received via electronic transmission from another system, or created by the system itself. Specifically, is information collected through technologies or other technologies used in the storage or transmission of information in identifiable form?

HR Smart collects data directly from users who have been granted access to the system. When a new VA employee is accessed, the employee record and their information are manually created and entered into HR Smart by the HR office using the information provided on the employment forms by the employee. Information is collected for the internal interfaces via Bidirectional using Secure File Transfer Protocol (SFTP) connections; unidirectional connections using SFTP; or Site to Site connection using VA internal network using SFTP. Information is collected for the external interfaces via Site-to-Site connections over business partner network using SSL bidirectional, or unidirectional connection using SFTP or Direct: Connect.

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

The VA HR line of business (LOB) maintains approved memoranda of understanding (MOU) and interconnection security agreements (ISA) for all interfacing organizations and systems.

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

These questions are related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.

1.4a Discuss whether and how often information stored in the system is checked for accuracy. Is information in the system checked against any other source of information (within or outside your organization) before the information is used to make decisions about an individual? For example, is there a computer matching agreement in place with another government agency? For systems that receive data from internal data sources or VA IT systems, describe the system checks to ensure that data corruption has not occurred during transmission.

Accuracy of information is validated through functional specification testing to validate data values and mappings, functional scenario-based testing to include both positive and negative testing, and file comparisons during parallel data entry and payroll phases.

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

Initial entry of information is done manually. When discrepancies arise, they are often discovered by the employee. Processes in place to prevent unauthorized access and changes include the use of row and role security. Row security refers to the access level such as VISN, POI, station, etc. Role security refers to what areas/pages they have access to such as HR Benefits, Payroll, Query, Quality

Reviewer, Manager, etc. One can have multiple roles and each role determines the permissions you have and actions you can take within the system. An HR Quality Reviewer is assigned to the system to also help ensure data accuracy.

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

- Title 38, United States Code, Sections 501(a), 1705, 1710, 1722, and 5317
- Information from SORN 171VA056A Human Resources Information Systems Shared Service Center (HRISS SSC)- VA: 38 U.S.C. 501(a); 38 U.S.C. 73; 38 U.S.C. 75 SEC 4202;5 U.S.C. Part III, Subparts D and E
- 5 U.S.C. 552, "Freedom of Information Act," c. 1967
- 5 U.S.C. 552a, "Privacy Act," c. 1974
- OMB Circular A-130, Appendix III, “Security of Federal Automated Information Systems”
- Information Technology Management Reform Act of 1996 (also known as the Clinger-Cohen Act)
- Federal Information Security Management Act (FISMA) of 2002
- OMB M-03-22, “OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002
- VA Directive 6502, VA Enterprise Privacy Program
- VA Directive 6300, Records and Information Management, and Handbook 6300.1, Records Management Procedures
- VA Handbook 6500, Risk Management Framework for VA Information Systems VA Information Security Program
- VA Policy NSCS-TG-025 Version 2
- NSA/Central Security Service Media Declassification and Destruction Manual
- Records Control Schedule 10-1, Section XIII-1 and Section XIII-2

- VA Form 0751, Information Technology Equipment Sanitization Certificate
- NIST SP 800-53

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

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

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

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

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

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

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

Follow the format below when entering your risk assessment:

Privacy Risk: HR Smart collects both Personally Identifiable Information (PII) and a variety of other Sensitive Personal Information (SPI). Due to the highly sensitive nature of this data, there is a risk that, if the data were accessed by an unauthorized individual or otherwise breached, then serious personal, professional, or financial harm may result for the individuals affected.

Mitigation: The HR Smart team has implemented required security and privacy controls for Federal information systems and organizations according to NIST SP 800-53 and VA Handbook 6500, Risk Management Framework for VA Information Systems. HR Smart employs a variety of security measures designed to ensure that information is not inappropriately disclosed or released. These measures include security and privacy controls for access control, awareness and training, audit and accountability, security assessment and authorization, configuration management, contingency planning, identification and authentication, incident response, maintenance, media protection, physical and environmental protection, planning, personnel security, risk assessment, system and services acquisition, system and communications protection, system and information integrity, and program management.

For all sensitive data / PII, cryptographic protections are used for both data at rest as well as data in transit (external and internal). HR Smart employs FIPS 140-2 validated encryption modules and supports FIPS 140-2 validated encryption mechanisms. Encryption of data at rest for all HR Smart operational environments is provided by the Pure storage array which is FIPS 140-2 certified and validated. All HR Smart backups are encrypted by Veritas Net Backup which is also FIPS 140-2 certified and validated.
Encryption of Information in transit between the customer and HR Smart is provided by an IPSec site-to- site VPN Tunnel over the Equinox Exchange fabric. The IPSec site to site VPN tunnel utilizes AES256 encryption and SHA1 authentication algorithm, which is a FIPS 140-2 compliant encryption mechanism. Also, all information sent between the HR Smart Application tiers is encrypted and protected by the use of TLS encryption, SSL certificates, machine keys, and software license keys. HR Smart is pursuing a FedRAMP Moderate ATO that is expected to be awarded in early 2022.

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.

- Name: Used to identify the employee and retained for employee HR record
- Social Security Number: Used as a unique employee identifier and retained for employee HR record
- Date of Birth: Used to identify employee age and retained for employee HR record
- Mailing Address: Used for communication and retained for employee HR record
- Phone Number(s): Used for communication and retained for employee HR record
- Email Address: Used for communication and retained for employee HR record
- Financial Account Information: Used to support payroll direct deposit
- Health Insurance: Used to provide employee benefits
- Race/Ethnicity: Voluntarily self-reported for employee HR record
- Gender: Used to identify employee gender and retained for employee HR record
- Military Status: Used to compute compensation and benefits
- VA Employment and Compensation Data: Used to maintain salary and benefit information; used to uniquely identify individuals.

- Next of Kin: Used to identify family member or relative.
- Emergency Contact: Used to identify the first person/s to contact in case of a medical or other crisis.

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

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

HR Smart is a human capital information system and does not include tools to perform complex analytical tasks resulting in, among other types of data matching, relational analysis, scoring, reporting, or pattern analysis.

2.2b If the system creates or makes available new or previously unutilized information about an individual, explain what will be done with the newly derived information. Will it be placed in the individual's existing record? Will a new record be created? Will any action be taken against or for the individual identified because of the newly derived data? If a new record is created, will the newly created information be accessible to Government employees who make determinations about the individual? If so, explain fully under which circumstances and by whom that information will be used.

In addition to the manual entry of data by employees, Quality Reviewers ensure the data quality through manual analysis and review.

2.3 How is the information in the system secured?
These questions are related to security and privacy controls SC-9, Transmission Confidentiality, and SC-28, Protection of Information at Rest.

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

HR Smart employs FIPS 140-2 validated encryption modules and supports FIPS 140-2 validated encryption mechanisms to ensure cryptographic protections for data at rest. Encryption of data at rest for all HR Smart operational environments is provided by the Pure storage array which is FIPS 140-2 certified and validated. All HR Smart backups are encrypted by Veritas Net Backup which is also FIPS 140-2 certified and validated.

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

HR Smart employs FIPS 140-2 validated encryption modules and supports FIPS 140-2 validated encryption mechanisms to ensure cryptographic protections for data at rest. Encryption of data at rest

for all HR Smart operational environments is provided by the Pure storage array which is FIPS 140-2 certified and validated. All HR Smart backups are encrypted by Veritas Net Backup which is also FIPS 140-2 certified and validated.

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

HR Smart employs FIPS 140-2 validated encryption modules and supports FIPS 140-2 validated encryption mechanisms to ensure cryptographic protections for data at rest. Encryption of data at rest for all HR Smart operational environments is provided by the Pure storage array which is FIPS 140-2 certified and validated. All HR Smart backups are encrypted by Veritas Net Backup which is also FIPS 140-2 certified and validated.

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information.

Describe any types of controls that may be in place to ensure that information is handled in accordance with the uses described above. ***Example: Describe if training for users of the project covers how to appropriately use information. Describe the disciplinary programs or system controls (i.e. denial of access) that are in place if an individual is inappropriately using the information.***

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

Principle of Transparency: Is the PIA and SORN, if applicable, clear about the uses of the information?

Principle of Use Limitation: Is the use of information contained in the system relevant to the mission of the project?
This question is related to privacy control AR-4, Privacy Monitoring and Auditing, AR-5, Privacy Awareness and Training, and SE-2, Privacy Incident response.

2.4a How is access to the PII determined?

- VA access form 9957 is submitted via the FSC ticketing portal for VA employees requesting access to the data. Additionally, numerous business roles including VA HR employees and Quality Reviewers restrict access to the data.

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

- Controls are in place to ensure data is used and protected in accordance with legal requirements, VA policies, and VA's stated purpose for using the data. Controls include mandatory training completion for all employees. Additionally, audits are performed to ensure information is accessed and retrieved appropriately. VA and IBM have implemented required security and privacy controls for Federal information systems and organizations according to NIST SP 800-53 and VA Handbook 6500, Risk Management Framework for VA Information Systems. HR Smart maintains a FedRAMP Moderate authorization to operate (ATO).

2.4c Does access require manager approval?

VA Staff requesting to a role in HR Smart that grants edit/update/view access to PII data must submit VA-Form 9957 that has been approved by the Servicing HR Officer for the HR Office they work under. The requests are submitted to the Center for Enterprise Human Resources Information Services (CEHRIS) Service Desk using the Pega Customer Relationship Management (CRM) case management solution. Service Desk staff reviews the requests for completeness and if the appropriate signatures are in place, grants access to the specific roles in HR Smart. A query can be produced with the name of the VA employees whose roles in HR Smart grants them edit/update/view access to PII data.

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

- A query can be produced with the name of the VA employees whose roles in HR Smart grants them edit/update/view access to PII data.

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

- VA and IBM have implemented required security and privacy controls for Federal information systems and organizations according to NIST SP 800-53 and VA Handbook 6500, Risk Management Framework for VA Information Systems.

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
- Personal Mailing Address
- Personal Phone Number(s)
- Personal Email Address
- Emergency Contact Information
- Financial Account Information
- Health Insurance Beneficiary Numbers
- Race/Ethnicity
- Gender
- Military History/Service Connection

- Next of Kin
- VA Employee and Compensation Data

3.2 How long is information retained?

In some cases, VA may choose to retain files in active status and archive them after a certain period of time. State active file retention periods, as well as archived records, in number of years, for the information and record types. ***For example, financial data held within your system may have a different retention period than medical records or education records held within your system, please be sure to list each of these retention periods****. The VA records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented. If the system is using cloud technology, will it be following the NARA approved retention length and schedule? This question is related to privacy control DM-2, Data Retention and Disposal.*

HR Smart data is retained online for all active and inactive VA employees at the General Datatech (GDT) Hosting data center. HR Smart follows the National Archives and Records Administration's (NARA) requirements and is retained for a period of 7 years.

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

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

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

HR Smart complies with all VA retention and disposal procedures specified in VA Handbook 6300 and VA Directive 6300. Records contained in the VA HR Smart SSC will be retained as long as the information is needed in accordance with a NARA-approved retention period. HRIS records are retained according to Record Control Schedule 10-1, https://www.archives.gov/files/records-mgmt/grs/grs01-1.pdf

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

HR Smart complies with all VA retention and disposal procedures specified in VA Handbook 6300 and VA Directive 6300. Records contained in the VA HR Smart SSC will be retained as long as the information is needed in accordance with a NARA-approved retention period. HRIS records are retained according to Record Control Schedule 10-1, https://www.archives.gov/files/records-mgmt/grs/grs01-1.pdf

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

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

The destruction of electronic data media complies with NCSC-TG-025 Version2/VA Policy. If a degausser is not available, the media is destroyed by smelting, pulverization or disintegration. Other IT equipment and electronic storage media are sanitized in accordance with procedures of the NSA/Central Security Service Media Declassification and Destruction Manual and certified that the data has been removed or that it is unreadable. Certification identifies the Federal Information Processing (FIP) item cleared. FIP equipment is not excessed, transferred, discontinued from rental or lease, exchanged, or sold without certification. The disposition authority is documented in Record Control Schedule 10-1, Section XLIII-1 and XLIII-2. Disposition instructions and procedures for electronic media are documented in NCSC-TG-025 Version2/VA Policy, VA Form 0751, Information Technology Equipment Sanitization Certificate. No records are disposed/destroyed without the approval of the facility's Record Control Manager. All records are disposed of in accordance with VA Policy and disposition authority (RCS 10-1), https://www.va.gov/vhapublications/RCS10/rcs10-1.pdf. Archived and retired records are maintained in accordance with VA Policy.

3.5 Does the system, where feasible, use techniques to minimize the risk to privacy by using PII for research, testing, or training?

Organizations often use PII for testing new applications or information systems prior to deployment. Organizations also use PII for research purposes and for training. These uses of PII increase the risks associated with the unauthorized disclosure or misuse of the information. Please explain what controls have been implemented to protect PII used for testing, training and research. This question is related to privacy control DM-3, Minimization of PII Used in Testing, Training and Research.

HR Smart's testing environment is included within the HR Smart authorization boundary, and all PII handled in the testing environment is protected by the same level of security and privacy controls implemented for the production environment. HR Smart does not use PII for research purposes and for training. All VA personnel data used in the HR Smart training environment is sanitized to prevent a person's identity from being connected with the information. All of the information contained in this system of records is used for official purposes of VA; all such uses of information are compatible with the purposes for which the information was collected. Furthermore, VA and IBM have implemented required security and privacy controls for Federal information systems and organizations according to NIST SP 800-53 and VA Handbook 6500, Risk Management Framework for VA Information Systems.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

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

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

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

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

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

Follow the format below:

Privacy Risk: The risk to maintaining data within the HR Smart system is that longer retention times increase the risk that information can be compromised or breached.

Mitigation: To mitigate the risk posed by information retention, HR Smart adheres to the VA Records Control Schedule (RCS) for each category or data it maintains. When the retention data is reached for a record, the HR Smart team will carefully dispose of the data by the determined method as described in question 3.4. All electronic storage media used to store, process, or access VA HR Smart records will be disposed of in adherence with the latest version of VA Handbook 6500.1, Electronic Media Sanitization.

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***
VA Time and Attendance (VATAS)	Necessary to exchange data files containing personnel data.	Name Social Security Number Personal Email Address VA Position and Compensation Data	Site to site connection using VA internal network using SFTP (Secure File Transfer Protocol)
VA Office of Inspector General (OIG)	The OIG Netezza system is a data repository that supports custom reporting capabilities required by the VA's Office of Inspector General for the purpose of conducting audits, research and related activities.	Name Social Security Number Date of Birth Personal Mailing Address Personal Phone Number(s) Personal Email Address Emergency Contact Information Financial Account Information Health Insurance Beneficiary Numbers Race/Ethnicity Gender	Interconnection is Unidirectional using SFTP

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*
		Military History/Service Connection Next of Kin VA Employee and Compensation Data	
VA Learning University Education Data Repository (VALU EDR)	Internal VA database that serves as the primary data source for VA TMS user profiles, maintaining strategic personal demographical data to support TMS operations.	Name Date of Birth Personal Email Address Military History/Service Connection VA Employee and Compensation Data	Interconnection is Unidirectional using SFTP
Veterans Health Administration Leadership &Workforce Development System (VHA LWD)	Information related to people, workforce, funding, leadership development, workforce development, personnel core competencies, senior executive information etc.	Name Date of Birth Personal Mailing Address Personal Phone Number Personal Email Address Emergency Contact Information Next of Kin Health Insurance Beneficiary Numbers VA Employee and Compensation Data Military History/Service Connection Gender	Interconnection is Unidirectional using SFTP
Department of Veterans Affairs (VA) Identity and Security Services (ISS)/ Department of Veterans Affairs (VA) Enterprise Shared Services Identity and Access Management (IAM)	IAM is using the MVI and Provisioning Service to provide onboarding support and self-service options for internal VA users for centralized creation, modification,	Name Address Date of Birth Personal Mailing Address Personal Phone Number Personal Email Address Military History/Service Connection VA Employee and Compensation Data	Interconnection is Unidirectional using SFTP

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*
	deletion and suspension for user accounts based on business processes and interactions defined by applications or systems. MVI and Provisioning Services integrate with Single Sign On internal (SSOi) service to allow users to SSO to the Provisioning Service web interface. MVI and Provisioning Services integrate with VA		
Enterprise Performance Management System (EPMS)	Workforce planning and performance management	VA Employee and Compensation Data	Interconnection is Unidirectional inbound to HR Smart using SFTP
Human Resources Personnel Accounting System (HRPAS)	Provides emergency notification service	Name Military History/Service Connection Social Security Number Personal Mailing Address Personal Phone Number Personal Email Address Military History/Service Connection VA Employee and Compensation Data Date of Birth Financial	Interconnection is Unidirectional outbound to HR Smart using SFTP

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*
		Account Information Gender	

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

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

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

Follow the format below:

Privacy Risk: There is a risk that information may be shared with unauthorized VA programs or systems.

Mitigation: Safeguards are implemented to ensure data is not sent to unauthorized VA organizations, including employee security and privacy training, and required reporting of suspicious activity. Use of secure passwords, access for need-to-know basis, Personal Identification Verification (PIV) Cards, Personal Identification Numbers (PIN), encryption, and access authorization are all measures that are utilized for the system.

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***
Defense Civilians Payroll System (DCPS) and Defense Finance and Accounting Service (DFAS)	Payroll data collected by VA and stored in HR Smart is transmitted to DFAS and used in DCPS to process VA payroll. Upon completion of	Name Social Security Number Date of Birth Personal Mailing Address Next of Kin Gender Military History/Service Connection	MOU/ISA	Site to Site connection over business partner network using SSL; bidirectional using SFTP

	processing, DFAS returns data to HR Smart for internal VA use.	VA Employee and Compensation Data		
United States Office of Personnel Management (OPM) Data Warehouse Program (DWP) EHRI/eOPF	The OPM Data Warehouse Program's Data Warehouse (DW) is a file containing records that covers a civilian federal employee's employment history. The OPM or VA HR LOB of human resources offices use these documents to make decisions about employee's right, benefits, and entitlements throughout their career.	Name Social Security Number Date of Birth Personal Mailing Address Social Security Number VA Employee and Compensation Data Military History/Service Connection Personal Email Address Emergency Contact Information Health Insurance Beneficiary Numbers Race/Ethnicity Gender	MOU/ISA	Site to Site connection over business partner network using SSL; bidirectional using Direct: Connect
DFAS myPay Web Application - Defense Finance and Accounting Service (DFAS) myPay Web Application Program Management Office (PMO)	HR Smart requires the use of the myPay Web Application's Thrift Savings Plan (TSP), Federal Employee Health Benefits (FEHB), personnel, and payroll information to expedite processing of	Name Social Security Number Date of Birth Personal Email Address Health Insurance Beneficiary Numbers	MOU/ISA	Site to Site connection over business partner network using SSL

	data associated with HR processing.			
MPDB - Defense Finance and Accounting Service (DFAS) myPay Master PIN (MPDB) Program Management Office (PMO)	myPay MPDB requires the use of HR Smart and e-mail address data to expedite processing of data associated with payroll processing.	Name Social Security Number Date of Birth Personal Email Address	MOU/ISA	Site to Site connection over business partner network using SSL
USA Staffing - United States Office of Personnel Management (OPM)	USA Staffing (OPM) is an online recruitment and applicant management system that facilitates screening and hiring of new employees. The system is accessible via an internet capable web browser. Applicant and certificate data are processed and stored. Data may also be transmitted electronically through a web services interface with an agency system	Name Social Security Number Date of Birth Personal Mailing Address Personal Email Address VA Employee and Compensation Data	MOU/ISA	Site to Site connection over business partner network using SSL
Intelligent Automation Platform (IAP)	IAP is a comprehensive automation solution which utilized unattended	• None (No VA sensitive, Data, PHI/ PII is transmitted)	MOU/ISA	Site to Site connection over business partner

	RPA to perform initial triage and handling of mail associated with Veterans benefits. This application processes scanned documents and additional functions that are performed include automated capture of data, Quality assurance (QA) of data and images as well as reporting on each of those components in a comprehensive Business Intelligence (BI) platform			network using SSL
Federal Employee Health benefits [FEHB] Data Hub FEHB Data Hub	FEHB Data Hub facilitates electronic submission of employee Health Benefit enrollment information. Federal Agencies electronically transmit Federal Employees Health Benefits	• Name • Social Security Number • Personal Mailing Address • Personal Email Address • VA Employee and Compensation Data	MOU/ISA	Site to Site connection over business partner network using SSL

	2809/2810 enrollment data to OPM-Macon.			
Monster Government Solutions (MGS) MHME (eClass360)	MGS (eClass360) is a Position Classification System that allows the VA to create position descriptions and functional statement and associated documentation . It allows for the creation, storage and routing of these documents for the appropriate business process flow.	• None (No VA sensitive, Data, PHI/ PII is transmitted)	MOU/ISA	Site to Site connection over business partner network using SSL

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: There is a risk that information may be shared with an external organization or agency that does not have a need or legal authority to access VA data.

Mitigation: Safeguards are implemented to ensure data is not shared with unauthorized organizations, including employee security and privacy training, and required reporting of suspicious activity. Use of secure passwords, access for need-to-know basis, Personal Identification Verification (PIV) Cards, Personal Identification Numbers (PIN), encryption and access authorization are all measures that are utilized for the system. Interconnection Security Agreements (ISA) and Memoranda of Understanding (MOU) are kept current and monitored closely to ensure protection of information.

Section 6. Notice

The following questions are directed at providing notice to the individual of the scope of information collected, the right to consent to uses of the information, and the right to decline to provide information.

6.1 Was notice provided to the individual before collection of the information? If yes, please provide a copy of the notice as an Appendix-A 6.1 on the last page of the document. Also provide notice given to individuals by the source system (A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register.) If notice was not provided, why not?

These questions are related to privacy control TR-1, Privacy Notice, and TR-2, System of Records Notices and Privacy Act Statements, and TR-3, Dissemination of Privacy Program Information.

6.1a This question is directed at the notice provided before collection of the information. This refers to whether the person is aware that his or her information is going to be collected. A notice may include a posted privacy policy, a Privacy Act statement on forms, or a SORN published in the Federal Register, Notice of Privacy Practice provided to individuals for VHA systems. If notice was provided in the Federal Register, provide the citation.

The list of VA Systems of Record Notice (SORNs), including the link to the HR Smart SORN, is located here:
https://www.oprm.va.gov/docs/Current_SORN_List_2_25_2022.pdf

Human Resources Information Systems Shared Service Center (HRIS SSC)-VA SORN: 171VA056A
HR Smart SORN: https://www.govinfo.gov/content/pkg/FR-2013-10-23/pdf/2013-24830.pdf

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

The Federal Register publication of the HR Smart System of Records Notice (SORN) is located here: http://www.gpo.gov/fdsys/pkg/FR-2013-10-23/pdf/2013-24830.pdf

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

HR Smart's Single Sign On page contains a privacy banner warning, please see the Appendix for further details.VA employees manually enter data upon initial use of the system. However, if there are any changes in the system, VA employees receive a Notification of Personnel Actions (SF-50) whenever HR processes an action in HR Smart.

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

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

Individuals can decline to provide information, and if so, will not be able to complete human resources and payroll activities necessary for employment.

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 data fields are required for human resources and payroll processing; however, individuals can voluntarily self-report personnel information including race, national origin, and ethnicity data, and disability.

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

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

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

<u>Principle of Transparency:</u> 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:

<u>Privacy Risk:</u> There is a risk that VA employees will not know that HR Smart collects,

maintains, and/or disseminates PII and other Sensitive Personal Information (SPI) about them.

Mitigation: HR Smart mitigates this risk by ensuring that it provides individuals notice of information collection and notice of the system's existence through the methods discussed in question 6.1.

Section 7. Access, Redress, and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about him or her.

7.1 What are the procedures that allow individuals to gain access to their information?

These questions are related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.

7.1a Cite any procedures or regulations your program has in place that allow access to information. These procedures, at a minimum, should include the agency's FOIA/Privacy Act practices, but may also include additional access provisions. ***For example, if your program has a customer satisfaction unit, that information, along with phone and email contact information, should be listed in this section in addition to the agency's procedures. See 5 CFR 294 and the VA FOIA Web page at http://www.foia.va.gov/ to obtain information about FOIA points of contact and information about agency FOIA processes.***

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

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

VA employees receive a basic account in PeopleSoft where they can view and update their personal information. Once the account is generated, an email is sent to individuals notifying them of their account.

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.

HR Smart is a self-service system and employees have access to their respective data. Since this is a self- service system, employees can access, redress and correct their own personal and personnel information, and they can review and update their respective HR information as necessary. As noted in section 7.1, all HR Smart users receive an account in PeopleSoft where they can view and update their personal information. Once the account is generated, an email is sent to individuals notifying them of their account. If there is data that cannot be updated via self-service, changes can be made by users going through their administration-level HR.

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.

As noted in section 7.1, all HR Smart users receive an account in PeopleSoft where they can view and update their personal information. Once the account is generated, an email is sent to individuals notifying them of their account. In addition, online training and help information are provided for employees that allow them to understand how they can correct their information. If there is data that cannot be updated via self-service, changes can be made by users going through their administration-level HR.

7.4 If no formal redress is provided, what alternatives are available to the individual?

Redress is the process by which an individual gains access to his or her records and seeks corrections or amendments to those records. Redress may be provided through the Privacy Act and Freedom of Information Act (FOIA), and also by other processes specific to a program, system, or group of systems. ***Example: Some projects allow users to directly access and correct/update their information online. This helps ensures data accuracy.***
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

The system is designed so that the self-service features are optional. Alternatively, employee managers and VA HR administrators can update information on the employee's behalf.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

Discuss what risks there currently are related to the Department's access, redress, and correction policies and procedures for this system and what, if any, steps have been taken to mitigate those risks. ***For example, if a project does not allow individual access, the risk of inaccurate data needs to be discussed in light of the purpose of the project. For example, providing access to ongoing law enforcement activities could negatively impact the program's effectiveness because the individuals involved might change their behavior.*** *(Work with your System ISSO to complete all Privacy Risk questions inside the document this section).*

Consider the following FIPPs below to assist in providing a response:
Principle of Individual Participation: Is the individual provided with the ability to find out whether a project maintains a record relating to him?

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

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

Follow the format below:

Privacy Risk: There is a risk that individuals whose records contain incorrect information may not receive notification of HR changes. Furthermore, incorrect information in an HR record could result in improper compensation or benefits.

Mitigation: HR Smart mitigates the risk of incorrect information in an individual's records by authenticating information and validating data accuracy using the resources discussed in question 1.5. Furthermore, VA employees will have access to their own individual online records using a username and password credentials, or by using Personal Identity Verification (PIV). Privileged users such as Human Resources Administrators and report generators will access online records other than their own, consistent with their authority and organizational affiliations using a username and password credentials. Select HR administrators have access to correct erroneous information as well, based on role.

Section 8. Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

8.1 What procedures are in place to determine which users may access the system, and are they documented?
These questions are related to privacy control AR-7, Privacy-Enhanced System Design and Development.

8.1a Describe the process by which an individual receives access to the system.

VA and IBM have developed, documented, and disseminated:

• An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
• Procedures to facilitate the implementation of the access control policy and associated access controls.

8.1b Identify users from other agencies who may have access to the system and under what roles these individuals have access to the system. Who establishes the criteria for what PII can be shared?

There are no users from other agencies that have access to HR Smart.

8.1c Describe the different roles in general terms that have been created to provide access to the system. For example, certain users may have "read-only" access while others may be permitted to make certain amendments or changes to the information.

HR Smart is a role-based HR system, therefore access to specific user roles are assigned based on what has been included on VA Form 9957 that has been signed by a Servicing HR Officer (or designee). The system can generate reports on all employees who have access to the data. The access control policy and procedure are reviewed and updated annually and upon material information system changes.
1) VA Office of Information Technology in coordination with the IBM PMO Team must authorize users of the HR Smart System, group and role membership, and access permissions for each account.
2) The HR Smart approvals must come from the user's business manager and must be confirmed through a need-to-know review conducted by the VA OIT.
3) The VA Program Management PIV Office creates, enables, modifies, disables, and removes information system accounts in accordance with VA Handbook 6510 Identity and Access Management and VA 0710 Personnel Security Standards.
4) The IBM HR Smart Administrators monitor and revalidate access through system and VA PMO provided reports.
5) The VA and HR Smart Access Administrators must notify account managers:1. When VA accounts are no longer required (within 90 days for inactive accounts)
    a. When users are terminated or transferred; and
    b. When individual information system usage or need-to-know changes.
6) HR Smart Administrators must authorize access to the HR Smart information system based on:
1.A valid access authorization.
7) Intended system usage; and
8) Any other unique attributes as required by the VA or associated missions/business functions;
9) The IBM Data Security and Privacy (DS&P) Access Administrators must review accounts for compliance with account management requirements at least monthly and for privileged accounts-monthly.

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—IBM was selected as the HR Smart operations and maintenance provider for the VA to build, operate, and maintain the system. HR Smart is hosted by the GDT hosting facility, with a primary

site in Dulles, Virginia and alternate site in Phoenix, Arizona. The TXP module is a SaaS solution of FedRAMP certified ServiceNow, located in in Culpepper, Virginia, and Miami, Florida. The system will not be used for managing contractor or volunteer elements of the VA labor force. VA maintains ownership of the collected data. Any contractors with access to the system complete VA's required security procedures and protocols to access it.

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

VA offers privacy and security training. Each program or system may offer training specific to the program or system that touches on information handling procedures and sensitivity of information. Please describe how individuals who have access to PII are trained to handle it appropriately. This question is related to privacy control AR-5, Privacy Awareness and Training.

VA and IBM provide security and privacy awareness training to information system users (including managers, senior executives, and contractors) as part of initial training for new users, when required by information system changes, and annually thereafter. All VA HR employees and contractors are required to take annual TMS training offered by VA. HR employees with access to HR Smart complete the VA Privacy and Information Security Awareness Rules and Behavior training annually, as required by VA Directive 6500.

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

8.4a If Yes, provide:

1. *The Security Plan Status:* Approved
2. *The System Security Plan Status Date:* 05/17/2023
3. *The Authorization Status:* Authorization to Operate (ATO)
4. *The Authorization Date:* 05/05/2022
5. *The Authorization Termination Date:* 05/04/2025
6. *The Risk Review Completion Date:* 04/21/2022
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* Moderate

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

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

N/A – A&A has been completed for HR Smart

Section 9 – Technology Usage

The following questions are used to identify the technologies being used by the IT system or project.

9.1 Does the system use cloud technology? If so, what cloud model is being utilized?

If so, Does the system have a FedRAMP provisional or agency authorization? If the system does use cloud technology, but does not have FedRAMP authorization, explain how the Cloud Service Provider (CSP) solution was assessed and what FedRAMP documents and processes were used for the assessment in order to comply with VA Handbook 6517. Types of cloud models include: Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Commercial off the Shelf (COTS), Desktop as a Service (DaaS), Mobile Backend as a Service (MBaaS), Information Technology Management as a Service (ITMaaS). This question is related to privacy control UL-1, Information Sharing with Third Parties.

***Note: For systems utilizing the VA Enterprise Cloud (VAEC), no further responses are required after 9.1**. (Refer to question 3.3.1 of the PTA)*

Yes. HR Smart is hosted by the Rectitude 369 hosting facility, with a primary site in Dulles, Virginia and alternate site in Phoenix, Arizona. The TXP module is a SaaS solution of FedRAMP certified (High) ServiceNow, located in in Culpepper, Virginia, and Miami, Florida.

9.2 Does the contract with the Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII? (Provide contract number and supporting information about PII/PHI from the contract). (*Refer to question 3.3.2 of the PTA) This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.*

Yes. VA's contract with IBM is: Task Order: GST36C10B23F0039 Contract No.: GS-35F-110DA. The contract with ServiceNow is with IBM.

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

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

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

Yes. TXP (ServiceNow) will collect required data for audit logging. All data will be owned by the VA.

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.

The IBM team develops and maintains the HR Smart solution to ensure organizational requirements are met. The IBM team has a contract and service level agreement in place with ServiceNow SaaS for the Talent Experience Platform (TXP) module. HR Smart operations and risk management are the responsibility of IBM.

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).

The system utilizes an RPA to automate ingestion of pay rate changes into the application. The user is able to email the RPA a PDF file with the pay rate change information for a salary schedule, the RPA will then perform business rule checks and processes the data into the system. The RPA does not process, exchange or store PII/PHI or any type of sensitive or controlled type of information.

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.

NEVALAN ORR

Digitally signed by NEVALAN ORR
Date: 2023.08.08 08:17:35 -04'00'

Privacy Officer, Nevalan Orr

LaToya N. Butler-Cleveland 204980

Digitally signed by LaToya N. Butler-Cleveland 204980
Date: 2023.08.23 23:48:40 -04'00'

Information System Security Officer, La Toya Butler-Cleveland

Ricardo Osborne

Digitally signed by Ricardo Osborne
Date: 2023.08.10 13:57:01 -04'00'

Information System Owner, Ricardo Osborne

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).

The list of VA Systems of Record Notice (SORNs), including the link to the HR Smart SORN, is located here: https://www.oprm.va.gov/docs/Current_SORN_List_2_25_2022.pdf

Human Resources Information Systems Shared Service Center (HRIS SSC)-VA SORN: 171VA056A

HR Smart SORN: https://www.govinfo.gov/content/pkg/FR-2013-10-23/pdf/2013-24830.pdf

HELPFUL LINKS:

Record Control Schedules:

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

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

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

National Archives (Federal Records Management):

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

VHA Publications:

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

VA Privacy Service Privacy Hub:

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

Notice of Privacy Practice (NOPP):

VHA Notice of Privacy Practices

VHA Handbook 1605.04: Notice of Privacy Practices