Privacy Impact Assessment for the VA IT System called:

Enterprise Performance Management System (ePerformance)

VACO

Human Capital Information Systems

Date PIA submitted for review:

October 11, 2022

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	*Harash Katyal*	*Harash.Katyal@va.gov*	*908-864-3107*
Information System Security Officer (ISSO)	*Steve Cosby*	*Steve.cosby@va.gov*	*919-201-4837*
Information System Owner	*Dominique A. Banks*	*Dominique.Banks@va.gov*	*202-632-8602*

Abstract

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

Enterprise Performance Management System (EPMS) ePerformance is a performance management system used for VA employees for their yearly performance plans to reduce need to have manual processes and printing and automatically moves employees plans over to the Federally required eOPF. ePerformance (Next Generation Cloud Platform) is a web-based Software as a service (SaaS) application that is hosted on a FedRAMP AWS (Amazon Web Service) approved cloud.

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.*
Enterprise Performance Management System (ePerformance) is hosted by the VHA HCM (Human Capital Management) organization.

B. *The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission.*
ePerforamnce is a SaaS cloud technology that is FedRAMP approved system and located on an AWS platform. Information is shared by the VA with the Northrop Grumman Cloud FedRAMP system and linked to eOPF through OPM. Controls are managed and secured through the AWS platform. FedRAMP controls are in place to manage PII to protect information. The system is classified as a moderate system with a magnitude of harm if privacy data is disclosed as a worst-case scenario for credit checks for effected employees.

C. *Indicate the ownership or control of the IT system or project.*
The IT system is controlled by the VA Central Office – Office of Chief Human Capital Officer.

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.*
ePerformance is an employee performance management system to assist VA employees with their performance plans. The expected number of individuals who will use the system is potentially all VA employees.

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

The general description of information is employee's performance plans, collecting these records for VA employees allows the system to automate their yearly performance plans to reduce need to have manual processes and printing.

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

ePerformance is a performance management system used for VA employees for their yearly performance plans to reduce need to have manual processes and printing and automatically moves employees plans over to the Federally required eOPF. ePerformance (Next Generation Cloud Platform) is a web-based Software as a service (SaaS) application that is hosted on a FedRAMP AWS (Amazon Web Service) approved cloud.

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.*

ePerforamnce is a SaaS operating within a FedRAMP approved system and located on an AWS platform. PII within the system is secured through controls that are managed and secured through the AWS platform.

3. Legal Authority and SORN

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

The legal authorities for collection of information are defined in the System of records notification (SORN) updated in 2018 and published to the federal register. This is in accordance with the Privacy Act and the System of Records Notice. https://www.govinfo.gov/ Legal authorities: 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.

VHALWD (Veterans Health Administration Human Capital Management-VA) System of Record Notification (SORN) is 161VA10A2, updated March 2018. - https://www.govinfo.gov/content/pkg/FR-2018-03-14/pdf/2018-05087.pdf

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 SORN does not require revision. The SORN covers cloud usage and storage.

D. System Changes

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

Will not result in changes to business processes.

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

Will not result in changes of technology.

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)

Other Data Elements:

- EmployeeID
- POID
- OrgCode
- OrgCodeDesc
- ActivityCode
- PositionTitle
- PositionNumber
- PayPlan
- Grade
- OccCode
- Supervisor
- Status
- Email
- ProbationaryStatus
- OrgLocation
- RatingOffical
- DateAssignedCurrentPosition
- Salary
- AppointmentType
- Service
- BargainingUnit
- SubAgency
- Region
- ComplexityLevel
- CostCode
- GradeStep
- NurseLevel
- AssignmentCode
- TitleCode
- FunctionalCode

- Routing
- DutyStation

PII Mapping of Components (Servers/Database)

ePerformance 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 ePerformance 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
HTM	Yes	Yes	• Social Security Number (Encrypted) • Name (first, last, middle) • Date of Birth • Organization • Salary Information • Position Title	Federal Government requirements for performance management.	FedRAMP security baselines such as Principle of least privilege, security controls, etc.
EMI	Yes	Yes	• Employee Name • Position Title	Federal Government requirements for performance management.	FedRAMP security baselines such as Principle of least privilege, security controls, etc.

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

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

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

The sources are received by VHALWD (Veterans Health Administration Leadership Workforce Development) VA from the HTM and EMI Databases.

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.

These sources are required to receive transmissions transmission from VA HRSmart, PAID, Active Directory, Nature of Action, Employee and Payroll to successfully run system procedures, these are then transferred to FedRAMP approved SaaS application.

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

The information currently creates reports and evaluations accessed through it.

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?

Received via electronic transmission from VA to the SaaS (Software as a Service) via secure SSL connection. Performance plan information is updated via the system twice per year for Federal employees and transfers over to OPM's eOPF (Electronic Official Personnel Folder). Information collected comes initially from other systems and also updated twice yearly during the performance period for VA employees.

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.

Not applicable.

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.*

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.

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.

The FedRAMP Northrop Grumman Cloud Platform system 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 for collection of information are defined in the System of records notification (SORN) updated in 2018 and published to the federal register. As prescribed in
VA Directive 6508, Implementation of Privacy Threshold Analysis and Privacy Impact Assessment. System Security Plan AP-01.1 Authority Collect. Organization shares information under the Routine Use Provisions of the Privacy Act. Through Privacy Impact Assessments, System Notices, Privacy System of Records Collection reviews, the organization ensure individuals are aware of the impact of privacy and describes the purposes of the information used. This is in accordance with the Privacy Act and the System of Records Notice. https://www.govinfo.gov/. SORN - 161VA10A2 - 2018-2025.

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.

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

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

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

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:
The FedRAMP approved NGCP (Northrop Grumman Cloud Platform) 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. 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 ePerformance applications is built using VA active directory roles and permissions.

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 for VA employee management system ePerformance and connects to OPM's eOPF. The following are the PII elements:
• Social Security Number (Encrypted) (Used as an identifier)
• Name (first, last, middle) (Used as an identifier)
• Date of Birth (Used as an identifier)
• Email Address (Used to contact employee)
• Organization (Used to identify organization for performance management and eOPF)
• Salary Information (Used to identify organization for performance management and eOPF)
• Position Title (Used to identify organization for performance management and eOPF)
Below are additional elements used to identify organization:

- EmployeeID
- POID
- OrgCode
- OrgCodeDesc
- ActivityCode
- PositionTitle
- PositionNumber
- PayPlan
- Grade
- OccCode
- Supervisor
- Status
- Email
- ProbationaryStatus
- OrgLocation
- RatingOffical
- DateAssignedCurrentPosition
- Salary
- AppointmentType
- Service
- BargainingUnit
- SubAgency
- Region
- ComplexityLevel
- CostCode

- GradeStep
- NurseLevel
- AssignmentCode
- TitleCode
- FunctionalCode
- Routing
- DutyStation

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.

Data is used for VA employee ePerformance system to manage and automate employee's yearly performance management appraisals and transfer to the Federal Government approved eOPF (Electronic Official Personnel Folder) for employee management.

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.

The system will automate updates to the employee's yearly performance management appraisals.

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?

All SSN's come from the HRSmart feed, via Secure File Transfer Protocols (SFTP). Title 38, United States Code, section 501a. The Social Security Numbers (SSNs) will be used or collected to uniquely identify the individual working within the VA. All SSN are encrypted while in transmission and at rest within the EPMS information system.

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

The ePerformance is hosted by the FedRAMP approved NGCP (Northrop Grumman Cloud Platform) which uses a number of security measures designed to identify SSNs and ensure there are protections in place.

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

The ePerformance is hosted by the FedRAMP approved NGCP (Northrop Grumman Cloud Platform) which uses a number of security measures designed to ensure PII/PHI is safeguarded in accordance with OMB Memorandum M-06-15.

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?

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.

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

The FedRAMP approved system 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.

2.4c Does access require manager approval?

The application is role specific and requires manager approval to receive roles to access information through active directory.

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

Safeguards include a VA baselined database, servers and recurring scans such as testing for servers, WASA scans for applications and database scans.

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

The ePerformance is hosted by the FedRAMP approved NGCP (Northrop Grumman Cloud Platform) which uses a number of security measures designed to identify SSNs and ensure there are protections in place.

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*

The following are the PII elements that are retained:

- Social Security Number (Encrypted)
- Name (first, last, middle)
- Date of Birth
- Email Address
- Organization
- Salary Information
- Position Title
- EmployeeID
- POID
- OrgCode
- OrgCodeDesc
- ActivityCode
- PositionTitle
- PositionNumber
- PayPlan

- Grade
- OccCode
- Supervisor
- Status
- Email
- ProbationaryStatus
- OrgLocation
- RatingOffical
- DateAssignedCurrentPosition
- Salary
- AppointmentType
- Service
- BargainingUnit
- SubAgency
- Region
- ComplexityLevel
- CostCode
- GradeStep
- NurseLevel
- AssignmentCode
- TitleCode
- FunctionalCode
- Routing
- DutyStation

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.*

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 (Senior Executive Service) 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 scheduled for 4 years based on GRS 5.2. An archive process is set to automatically remove the data on expiration. VA GRS 5.2 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)?

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?

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. 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.

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

The retention period is scheduled for 4 years based on GRS 5.2. An archive process is set to automatically remove the data on expiration. VA GRS 5.2 has Records Management Responsibilities for developing policies and procedures for effective and efficient records management throughout VHA.

GRS 4.3 (superseded to 5.2) - https://www.archives.gov/files/records-mgmt/grs/grs05-2.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.

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. 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 are encrypted and 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 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 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 baselined database, servers and Cybersecurity Operations Center recurring scans such as testing for servers, WASA scans for applications and database scans.

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

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

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

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

<u>Principle of Minimization:</u> 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?

<u>Principle of Data Quality and Integrity:</u> 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:

<u>Privacy Risk:</u>
Due to the sensitive nature of this data, there is a risk that this information could be retained longer than necessary.

<u>Mitigation:</u>
Procedures will be enforced using technical and managerial control mechanisms including the Records Control Schedule (RCS) 10-1 VA guidance and having a disposal authority and log files for past and future suspense notices. The retention period is scheduled for 4 years. An archive process is set to automatically remove the data on expiration.

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***
N/A			

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:

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 GRS 5.2 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 are all in place and updated on the VA approved schedule.

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***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted)with the Program or IT system***	***List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can***	***List the method of transmission and the measures in place to secure data***

	office or IT system		***be more than one)***	
eOPF	Extracts from the ePerformance system to the OPM system	Employee Name, SSN, Performance Information	Signed MOU/ISA/ICD for both agencies.	IBM Direct Connect
Next Generation Cloud Platform (NGCP)	Extracts from the VA VHALWD system to NGCP to the OPM eOPF system	Social Security Number (Encrypted) Name (first, last, middle) Date of Birth Email Address Organization Salary Information Position Title	Signed MOU/ISA/ICD for both agencies.	S3 Secure

5.2 <u>PRIVACY IMPACT ASSESSMENT: External sharing and disclosure</u>

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:

<u>Privacy Risk:</u>
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.

<u>Mitigation:</u>
Procedures will be enforced using technical and managerial control mechanisms including following the 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 are all in place and updated on the VA approved schedule.

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.

Yes, notices are provided. See examples below. A SORN is also registered for the system of records notice per privacy standards. https://www.govinfo.gov/content/pkg/FR-2018-03-14/pdf/2018-05087.pdf . SORN - 161VA10A2/ 83 FR 11297 Veterans Health Administration Human Capital Management-VA.

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

Copy of notice removed per accessibility issues. The system uses VA SSO prior to the users accessing the system, inheriting warning and privacy notification of system use from the organization.

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.

Upon logging into computers and browsing to the portal, a notification pops up throughout the user experience.

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 PRIVACY IMPACT ASSESSMENT: Notice

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

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

Principle of Transparency: *Has sufficient notice been provided to the individual?*

Principle of Use Limitation: *Is the information used only for the purpose for which notice was provided either directly to the individual or through a public notice? What procedures are in place to ensure that information is used only for the purpose articulated in the notice?*
This question is related to privacy control TR-1, Privacy Notice, AR-2, Privacy Impact and Risk Assessment, and UL-1, Internal Use.
Follow the format below:

Privacy Risk:
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:
A privacy notice must be acknowledged each time someone visits our intranet application portal.

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.***

Employees update their data through either the ePerformance performance management system or the HRSmart and PAID systems. Employees work with their HR office for procedures for updating their information. Employees can access HRSmart at https://ssologon.iam.va.gov/CentralLogin/. Additional information can be found in PIA's of the HRSmart system.

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).

Not applicable.

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.

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 either the ePerformance performance management system or the HRSmart and PAID systems. Employees work with their HR office for procedures for updating their information. Employees can access HRSmart at https://ssologon.iam.va.gov/CentralLogin/. Additional information can be found in PIA's of the HRSmart system. To request a FOIA request outside of VA, see instructions at http://www.foia.gov/how-to.html

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 either the ePerformance performance management system or the HRSmart and PAID systems. Employees work with their HR office for procedures for updating their information. Employees can access HRSmart at https://ssologon.iam.va.gov/CentralLogin/. Additional information can be found in PIA's of the HRSmart system. To request a FOIA request outside of VA, see instructions at http://www.foia.gov/how-to.html

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.

Employees update their data through either the ePerformance performance management system or the HRSmart and PAID systems. Employees work with their HR office for procedures for updating their information. Employees can access HRSmart at https://ssologon.iam.va.gov/CentralLogin/. Additional information can be found in PIA's of the HRSmart system. To request a FOIA request outside of VA, see instructions at http://www.foia.gov/how-to.html

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:
<u>Principle of Individual Participation:</u> Is the individual provided with the ability to find out whether a project maintains a record relating to him?

<u>Principle of Individual Participation:</u> 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?

<u>Principle of Individual Participation:</u> 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:

<u>Privacy Risk:</u>
There is a risk that individuals are unaware of how to access or correct their information in the system.

<u>Mitigation:</u>
Employees update their data through either the ePerformance performance management system or the HRSmart and PAID systems. Employees work with their HR office for procedures for updating their information. Employees can access HRSmart at https://ssologon.iam.va.gov/CentralLogin/. Recurring employee training and HR communication is used to mitigate this challenge.

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.

The ePerformance application are built using VA active directory roles and permissions. Employees receive permission through their organization and the HCM helpdesk.

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?

A federal employee, can see their own record. If I were a manager, I would be able to see the information of my employees. For example in 2018-2020, the ePerformance system brought on OIT staff.

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.

The system admins setup and provide access, permissions and coordinated with the training arm of the VA to update staff on how-to steps using their PIV cards.

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.

- System end users are federal employees. Northrop Grumman contractors manage the system through the AWS FedRAMP SaaS.
- All NDA’s have been signed for contractors.

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.

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:* 5/25/2022
3. *The Authorization Status:* Authorized
4. *The Authorization Date:* 11/20/2020
5. *The Authorization Termination Date:* 11/19/2023
6. *The Risk Review Completion Date:* 5/25/2022
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* Moderate
8.

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.***

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)*

EPMS is hosted under the Next Generation Cloud Platform (NGCP – eMASS ID: 902) / Peraton – Amazon Web Services (AWS), managed by Peraton under a FedRAMP certified package (Package ID: FR1716961549).

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.*

The NGCP adheres to all of the NIST standards for security, but the customer has the ultimate responsibility for any PII.

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.

The NGCP doesn't collect any information about what is going on inside the application. We are the shell, and we do not have any access to what occurs inside the application.

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.

NGCP as the CSP ensures risks are managed and handled per FISMA requirements – reporting to the VA as an organization of these monitored risks for any further escalation.

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 does not use RPA.

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**

ID	Privacy Controls
DM-1	Minimization of Personally Identifiable Information
DM-2	Data Retention and Disposal
DM-3	Minimization of PII Used in Testing, Training, and Research
IP	**Individual Participation and Redress**
IP-1	Consent
IP-2	Individual Access
IP-3	Redress
IP-4	Complaint Management
SE	**Security**
SE-1	Inventory of Personally Identifiable Information
SE-2	Privacy Incident Response
TR	**Transparency**
TR-1	Privacy Notice
TR-2	System of Records Notices and Privacy Act Statements
TR-3	Dissemination of Privacy Program Information
UL	**Use Limitation**
UL-1	Internal Use
UL-2	Information Sharing with Third Parties

Signature of Responsible Officials

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

Harash B. Katyal 681075

Digitally signed by Harash B. Katyal 681075
Date: 2023.04.26 09:07:05 -04'00'

Privacy Officer, Harash Katyal

Steve M. Cosby 223809

Digitally signed by Steve M. Cosby 223809
Date: 2023.04.26 10:22:16 -04'00'

Information System Security Officer, Steve Cosby

Dominique A. Banks 747748

Digitally signed by Dominique A. Banks 747748
Date: 2023.05.23 16:12:20 -04'00'

Information System Owner, Dominique A. Banks

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).

VHALWD (Veterans Health Administration Human Capital Management-VA) System of Record Notification (SORN) is 161VA10A2, updated March 2018. - https://www.govinfo.gov/content/pkg/FR-2018-03-14/pdf/2018-05087.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