Privacy Impact Assessment for the VA IT System called:

AINS – eCase -E

Enterprise Human Resources Information Services (EHRIS)

Date PIA submitted for review:

June 7, 2021

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Jacquelyn Filkins	Jacquelyn.Filkins@va.gov	607-664-6964
Information System Security Officer (ISSO)	Karen A. McQuaid	Karen.McQuaid@va.gov	708-483-5311
Information System Owner	Travis L. Frayer	Travis.Frayer@va.gov	202-461-7906

Abstract

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

The application is called eCase, provided by a commercial company called AINS. eCase is a Commercial Off-The-Shelf (COTS) product to be hosted in a FedRAMP cloud environment, maintained and operated by AINS. With eCase, the Safety and Workers' Compensation Information Management System (SWIMS) has been created to be an enterprise-wide Safety Policy management system, that tracks and reports workplace environments, construction projects, fire code adherence, safe handling and storage of hazardous materials, ergonomically correct work practices, and more. VA staff of various departments submit cases through a user-friendly web interface, with the ability to generate reports to capture safety performance measures.

Overview

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

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

As mentioned in the abstract, SWIMS has been created to be an enterprise-wide Safety Policy management system on the eCase SaaS platform. The product will allow a variety of tasks required for the planning, orchestration and execution of safety programs across the VA. It manages health and safety policies, systems, standards, and records. It involves incorporating VA health and safety activities and programs into other VA business processes. Part of ensuring a safe workplace is education of potential hazards presented in an individual's personal workspace. To this end, it is necessary for the platform to have basic demographic information about VA employees that they may be assigned the correct trainings and that credit is received for their completion. Any VA employee and contractors that fills out an incident report in DOL which is sent to eCase. The typical client is the VA employee that has a workplace incident.

There is a cloud service provider contract with AINS via B3 Group, Inc and the contract number is VA118-16-D-1008 36C10B20N10080040. This network will have a secure site-to-site connection with the VA. VA employees will only be able to access the SWIMS web portal from the VA Network.

The FedRAMP compliant data center/cloud environment owned and operated by AINS will use a variety of technologies to deliver continuous uptime and availability. eCase is housed in one site – located in Virginia. The operating system used is Windows 2016 and the database is created on Structured Query Language (SQL) 2014/2017. All windows virtual images are created using VMWare hypervisor. A hypervisor, also known as a virtual machine monitor or VMM, is software that creates and runs virtual machines (VMs). A hypervisor allows one host computer to support multiple guest VMs by virtually sharing its resources, such as memory and processing. The system is protected with SonicWALL firewall. All the security services on the firewall are enabled which includes Internet Protocol Security (IPSec), Malicious code protection, anti-malware protection, content filtering. The system is backed up daily (incremental) and weekly full backup. Storage Area Network/Network Attached Storage (SAN/NAS) storages are used for backup storage. Multiple virtual Local Area Networks (LANs) are created to separate different customers instances.

eCase application presents itself as a web-based application which is installed on Internet Information Services (IIS) web server. eCase is case management system specifically designed to be highly configurable to meet a broad range of business needs. The eCase platform is already being used by the VA to fulfill HR requirements such as track and report employee conduct issues, disciplinary actions, performance improvement plans (PIPs), grievances and appeals, informational and reasonable accommodation requests, terminations and miscellaneous leave issues.

The authority to collect this information is derived from SORN: https://www.opm.gov/information-management/privacy-policy/sorn/opm-sorn-govt-1-general-personnel-records.pdf, OPMGOVT-1, 5 U.S.C. 1302, 2951, 3301, 3372, 4118, 8347, and Executive Orders 9397, 9830, and 12107.

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.

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

☒ Name
☒ Social Security Number
☒ Date of Birth
□ Mother's Maiden Name
☒ Personal Mailing Address
☒ Personal Phone Number(s)
□ Personal Fax Number
□ Personal Email Address
□ Emergency Contact Information (Name, Phone Number, etc. of a different individual)
□ Financial Account Information
□ Health Insurance Beneficiary Numbers Account numbers
□ Certificate/License numbers
□ Vehicle License Plate Number
□ Internet Protocol (IP) Address Numbers
□ Current Medications
□ Previous Medical Records
□ Race/Ethnicity
□ Tax Identification Number
□ Medical Record Number
☒ Other Unique Identifying Information (list below)

- Employee ID (HRPAS)
- Incident Case Number
- Gender
- Date of Incident
- Zip Injury occurred
- Facility of Employment
- Occupational Series Code
- Name of Physician (if seen due to incident, OSHA 301 form)
- Treatment Address (if address different than place of employment and if seen due to incident, OSHA 301 form)
- OSHA 301 Case Number
- Date Hired

PII Mapping of Components

AINS – eCase -E consists of one key component. Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by **AINS – eCase -E** and the reasons for the collection of the PII are in the table below.

PII Mapped to Components

PII Mapped to Components

Database Name of the information system collecting/storing PII	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
SWIMSprodDB	Yes	Yes	DOB Name Address Phone Number Employee ID	Used to validate and identify employee	All PII is encrypted while in use and stored, and only available to certain users. FedRAMP compliant encryption

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

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

Describe why information from sources other than the individual is required. For example, if a program's system is using data from a commercial aggregator of information or data taken from public Web sites, state the fact that this is where the information is coming from and then in question 1.3 indicate why the system is using this source of data.

If the system creates information (for example, a score, analysis, or report), list the system as a source of information.
This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

There is an interface from VA's authoritative source Human Resources Payroll Applications Services (HRPAS) to eCase that imports the data fields identified. eCase is not the authoritative data source for VA employees – only HRPAS. It does collect basic user file information from VA employees and contractors. Additionally, eCase will be ingesting a file from the Department of Labor (DOL) that contains a listing of Occupational Safety and Health Administration (OSHA) related information.

The interface from the VA authoritative source ensures data integrity and eliminates erroneous employee data entry.

1.3 How is the information collected?

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

If the information is collected on a form and is subject to the Paperwork Reduction Act, give the form's OMB control number and the agency form number.
This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

The information is collected via electronic transmission upon request from HRPAS and the DOL. by eCase. eCase does collect basic user file information from VA employees and contractors.

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

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

If the system checks for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract.
This question is related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.

eCase is validated against the VA's authoritative system, HRPAS, for personnel records. When an employee of the VA is searched for to either assign training or to check on the status of their training, eCase sends a request to HRPAS to validate their demographic information such as name, DOB, etc. to confirm their identity.

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 authority to collect this information is derived from SOR: https://www.opm.gov/information-management/privacy-policy/sorn/opm-sorn-govt-1-general-personnel-records.pdf - OPMGOVT-1, 5 U.S.C. 1302, 2951, 3301, 3372, 4118, 8347, and Executive Orders 9397, 9830, and 12107.

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.

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: The Privacy risk for this system is an individual record could be accessed without the proper authorization.

Mitigation: To mitigate against this risk, the VA is requiring the use of FIPS 140-2 encryption modules and 2 Factor Authorization (2FA). Only VA HR personnel will have access to the system and must utilize a PIV to gain access. All contractors and vendors are under contract or agreements to ensure confidentiality remains in place. Roles and responsibilities will be regularly audited by system administrators and supervisors. These roles dictate the data that individuals are privileged to see.

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.

Internal to VA:
The SPI is unique and is utilized to track adherence of each employee to the safety policies throughout the VA ensuring compliance. VA has a requirement for a new VA System of Record for workers' compensation and occupational safety and health data to satisfy the Occupational Safety

and Health (OSH) Act of 1970, Section 19(a)(3) and (5). This law requires Federal agencies to keep adequate records of all occupational accidents and illnesses for proper evaluation and necessary corrective action, and to provide access to those records and reports to the Secretary of Labor when requested

External to VA:
No external connections exist to share data.

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

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

If the system creates or makes available new or previously unutilized information about an individual, explain what will be done with the newly derived information. Will it be placed in the individual's existing record? Will a new record be created? Will any action be taken against or for the individual identified because of the newly derived data? If a new record is created, will the newly created information be accessible to Government employees who make determinations about the individual? If so, explain fully under which circumstances and by whom that information will be used.
This question is related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information

Online eCase (e.g. SWIMS modules) reporting tools are inherently part of the information system and utilized to analyze audits taking place in workplace environments, develop quantitative analysis, and generate a workplace level risk assessment matrix. No new information will be added to any individual’s record nor reported for any specific individual. Third party tools are not utilized to perform any data analysis for reporting.

2.3 How is the information in the system secured?

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

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

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

AINS eCase -E and its system components such as the hypervisor for the virtual machine is protected with SonicWALL firewall. All the security services on the firewall are enabled which includes Internet Protocol Security (IPSec), malicious code protection, anti-malware protection, content filtering. The system is backed up daily (incremental) and weekly full backup. All data at rest is encrypted with BitLocker. This includes SSN which is stored in database, and it is protected using

SQL TDE encryption. Data in transit is encrypted via TLS 1.2. All incoming and outgoing traffic (data in transit) from the web server is encrypted and transmitted through a VA Trusted Internet Connection (TIC). The site may only be accessed by user's on the VA network, either physical connection or through the usage of a Virtual Private Network (VPN) connection due to a site-to-site tunnel between AINS' data center and the VA Network.

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

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

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

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

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

The system has role-based access. System administrators will ensure safeguards for the PII by granting higher level permissions to department level supervisors. These empowered supervisors will grant roles and responsibilities to individuals as they deem necessary. The supervisors will be informed on the procedure to do so with thorough training documentation. Each department will review the roles, responsibilities, and permissions at regular intervals. Access to PII is monitored through system event logs. These logs are accessible by the System administrators and can be reviewed as needed.

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

ID

Employee ID (HRPAS), Incident Case Number, Gender, Date of Incident, Zip Injury occurred, Facility of Employment, Occupational Series Code, Name of Physician (if seen due to incident, OSHA 301 form), Treatment Address (if address different than place of employment and if seen due to incident, OSHA 301 form), OSHA 301 Case Number, Date Hired

3.2 How long is information retained?

In some cases VA may choose to retain files in active status and archive them after a certain period of time. State active file retention periods, as well as archived records, in number of years, for the information and record types. For example, financial data held within your system may have a different retention period than medical records or education records held within your system, please be sure to list each of these retention periods. If the system is using cloud technology, will it be following the NARA approved retention length and schedule?

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

The information housed in eCase is only related to an employee's safety. Information is retained for at least 5 years in alignment with guidance in the VA Handbook 6300.1 – Records Management Procedures and VA Directive 6300 – Records and Information Management. In addition, per the contract VA118-16-D-1008 36C10B20N10080040, section 5.2.1, "…Support five-year data retention requirements," section 5.6. eCase complies with VA RCS 10-1, Item Number 3075.10 (b) for record retention. A VA records management officer is being consulted to verify applicability and usage of data retention periods.

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

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

This is a cloud-based system where data is not housed within the VA network/authorization boundary. eCase complies with VA RCS 10-1, Item Number 3075.10 (b) (https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf) for record retention. The vendor complies with FedRAMP and NARA requirements for data retention as well. VA has a contract (VA118-16-D-1008 36C10B20N10080040) with the vendor (B3 Group, Inc & AINS) on specific language related with data retention and the vendor's responsibility to ensure VA data is not compromised.

3.4 What are the procedures for the elimination of SPI?

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

If the contract ends with B3 Group, Inc. the system will be decommissioned. Although the system will no longer be available to the VA, the VA is to receive all information/data stored in eCase. All data stored on the VA's behalf by AINS will be returned to the VA and purged from AINS servers. Data is ONLY destroyed at the request of VA or termination of the existing contract.

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

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

Yes, the system does use techniques to minimize the risk of privacy of using PII for research, testing, or training. Training/Testing for eCase is completed in a test environment with mock data. Only those with permissions to eCase can access the system and utilize the system based on the role given. eCase contains a log of every server request. This feature will aid in the audit of eCase. ECase PII is not used for research and training.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

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

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

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

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

Principle of Data Quality and Integrity: *Has the PIA described policies and procedures for how PII that is no longer relevant and necessary is purged?*

This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal.

Follow the format below:
Privacy Risk: There is a risk that the information maintained by eCase could be retained for longer than is necessary to fulfill the VA mission. Records held longer than required are at greater risk of being unintentionally released, breached, or exploited for reasons other than what is described in the privacy documentation associated with the information.

Mitigation: To mitigate the risk posed by information retention, eCase adheres with FedRAMP and NARA requirements for data retention. Information is retained for at least 5 years in alignment with guidance in the VA Handbook 6300.1 – Records Management Procedures and VA Directive 6300 – Records and Information Management. VA has a contract (VA118-16-D-1008 36C10B20N10080040) with the vendor (B3 Group, Inc & AINS) on specific language related with data retention and the vendor's responsibility to ensure VA data is not compromised. eCase complies with VA RCS 10-1, Item Number 3075.10 (b) for record retention. eCase project staff will periodically review data retention thresholds such as the 5-year requirement and discuss options with VA before purging data. Data will be transferred to VA at their request upon completion of the contract.

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?

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 shared/received with the Program Office or IT system***	***Describe the method of transmittal***
Human Resources and Payroll Accounting System (HRPAS)	To ensure the adherence of each employee to the safety policy throughout the VA ensuring compliance.	1. Employee Name 2. Employee ID 3. Employee Entry on Duty (EOD) 4. Employee Position Title 5. Employee Pay Plan 6. Employee Series 7. Employee Grade 8. Bargaining Unit Status 9. Appointment Type 10. Employee Department 11. Personnel Office Identifier (POID) 12. Station Number 13. Veterans Integrated Service Network (VISN) 14. Cost Center 15. Organization Code 16. Supervisor Name 17. Supervisor Employee ID 18. Supervisor Position Number 19. Employee Position Number 20. Reports To 21. Union Code	Electronic transmittal via file transfers and User Interface (UI).

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

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

Follow the format below:
Privacy Risk: The Privacy risk for this system is an individual record could be accessed without the proper authorization.

Mitigation: Each user that has access to the system is assigned a role and permission. This role and permissions are based on the Active Directory account associated with the individual. Users with only valid PIV cards can access the system via the Single Sign On internal (SSOi) method.

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.
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 received with	*List the purpose of information being received from the specified*	*List the specific PII/PHI data elements that are received 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*

	program office or IT system			
Department of Labor (DOL)	Health and Safety audits.	Last Name First Name DOB Email Address Workplace Incident Information Incident Treatment Site Treating Physician	MEMORANDUM OF UNDERSTANDING BETWEEN OFFICE OF WORKERS' COMPENSATION PROGRAMS (OWCP) DIVISION OF FEDERAL EMPLOYEES' COMPENSATION (DFEC) And DEPARTMENT OF VETERANS' AFFAIRS (DVA)	DOL will drop file in AITC via SFTP. Vendor will retrieve file and ingest it into eCase. Data is protected via TLS 1.2 and FIPS 140-2 encryption.

This data is ONLY received via SFTP and ingested into eCase. At no point is data sent back to DOL from VA.

If specific measures have been taken to meet the requirements of OMB Memoranda M-06-15 and M-06-16, note them here.

To protect Veteran personally identifiable information (PII) the following activities occur as part of the overall information assurance activities:

1. The information with each application is categorized in accordance with FIPS 199 and NIST SP 800-60. As part of the categorization any PII is identified.
2. The VA has policies which direct and guide the activities and processes performed by the VA. The policies are periodically reviewed to ensure completeness and applicability.
3. The NIST SP 800-53 controls are selected based on the categorization. The controls provide protection for veteran PII while, used developed or stored by an application or IT system, physically transported, between facilities, least privilege, stored offsite, or transmitted between IT centers.
4. Internal protection is managed by access controls such as user IDs and passwords, two-factor authentication, in addition: awareness and training, encryption, auditing, and internal network controls. Remote protection is provided by remote access control, authenticator

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:
Privacy Risk: The privacy risk to VA is negligible. The file received at AITC via DOL SFTP drop may contain malicious content.

Mitigation: All files received are scanned at AITC for potential threats before entry into the eCase system.

Section 6. Notice

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

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

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

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

Describe how the notice provided for the collection of information is adequate to inform those affected by the system that their information has been collected and is being used appropriately. Provide information on any notice provided on forms or on Web sites associated with the collection. This question is related to privacy control TR-1, Privacy Notice, and TR-2, System of Records Notices and Privacy Act Statements, and TR-3, Dissemination of Privacy Program Information.

The Department of Veterans Affairs provides notice of information collection in several additional ways. The initial method of notification is in person during individual interviews by VA employees or VA supervisors or in writing via the Privacy Act statement on forms and applications completed by the individual. eCase does not collect any PII or PHI directly from the individual. Records provided to eCase by the DOL were entered by user through the ECOMP Web Portal. At the time of entry, they are notified that the information may be transmitted to departments internal to the VA for regulatory and investigative purposes.

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

Once an individual accepts the offer to become a VA employee, the employee right to decline is waived to have employee information entered in a HR system. If an individual rejects a job offer, he/she can do so verbally or via written communication.

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

With acceptance of the offer to become a VA employee, the employee consents to uses of the information. The individual has the right to decline the offer and thereby declining the consent.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

Describe the potential risks associated with potentially insufficient notice and what steps, if any, are currently being taken to mitigate those identified risks.

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

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

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

Follow the format below:
Privacy Risk: Insufficient notice of information being shared may put an individual in a situation that they are not prepared for and breach their privacy rights and trust. Information collected is from secured information systems with appropriate security controls in place. Individuals consent to their information being utilized for the purpose of VA safety measures during initial VA hire.

Mitigation: Information being collected in the AINS – eCase -E system is not being disseminated/shared and therefore cannot risk insufficient notice.

Section 7. Access, Redress, and Correction

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

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

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

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

If the system is not a Privacy Act system, please explain what procedures and regulations are in place that covers an individual gaining access to his or her information.
This question is related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.

The employee can access their information thru the VA authoritative data sources, HRPAS and the DOL, following the guidelines outlined by HRPAS and the DOL. The PII/PHI collector follows the guidance of Office of Management and Budget (OMB) Circular A-130 when processing Privacy Act/FOIA requests from individuals. Procedures for adhering to a FOIA request are outlined in VA Handbook 6300.4: Procedures for Processing Requests for Records Subject to the Privacy Act.

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.

The employee can request corrections of their data through the VA authoritative data sources, HRPAS and the DOL, following the guidelines outlined by HRPAS and the DOL.

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.

eCase only collects information from VA systems such as HRPAS. VA employees do not correct their information in eCase.

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

Redress is the process by which an individual gains access to his or her records and seeks corrections or amendments to those records. Redress may be provided through the Privacy Act and Freedom of Information Act (FOIA), and also by other processes specific to a program, system, or group of systems.
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

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

This system is a case management tool. It is not the VA authoritative source for HR; however, it will receive employee information from VA's authoritative data source, HRPAS. If employee notices a discrepancy, they can contact their supervisor. The supervisor can submit the change via HR·Smart or by contacting the HR staffing representative.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

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

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

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

Follow the format below:
Privacy Risk: If there is a discrepancy in the employee data, it can result in misidentification of safety policy participants.

<u>Mitigation:</u> If employee notices a discrepancy, they can contact their supervisor. The supervisor can submit the change via HR Smart or by contacting the HR staffing representative.

Section 8. Technical Access and Security

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

8.1 What procedures are in place to determine which users may access the system, and are they documented?

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

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

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

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

The system has role-based access. System administrators will ensure safeguards for the PII by granting higher level permissions to department level supervisors. These empowered supervisors will grant roles and responsibilities to individuals as they deem necessary. The supervisors will be informed on the procedure to do so with thorough training documentation. Each department will review the roles, responsibilities, and permissions at regular intervals. Access to PII is monitored through system event logs. These logs are accessible by the System administrators and can be reviewed as needed.

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. VA Contractors developed and maintain the system. Contracts are reviewed annually at a minimum. The contractors who provide support to the system are required to complete annual VA Privacy and Information Security and Rules of behavior training via the VA's TMS. All contractors are cleared using the VA background investigation process and must obtain a Moderate Background Investigation (MBI) or full BI if they will be accessing PII or PHI. Aside from the VA contractor requirements already specified in this section, contractors are not specifically required to sign additional NDAs or confidentiality agreements. Contractors are required to comply with all VA policy regarding access to systems and PII. Per the contract (VA118-16-D-1008 36C10B20N10080040), section 5.1.6, contractors will complete annual TMS training requirements and submit certificates of completion to the COR to ensure proper training and awareness are enforced to act as deterrent to unauthorized disclosure of VA data.

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.

There is no additional security training for AINS – eCase -E personnel over and above that required by VA.VA ensures that all personnel provide certificates of training annually for VA Privacy and Information Security Awareness training. All the AINS – eCase -E project team is required to sign a Rules of Behavior agreement prior to being given access to the system. Additionally, the Rules of Behavior is required to be reviewed and signed annually by each user. Annual training for the National Rules of Behavior is performed through the Talent Management System (TMS). There are two versions of the National Rules of Behavior: one for VA employees and one for contractors.

Following are the definitions of VA employee and VA Contractor:

- VA Employees - VA employees are all individuals who are employed under title 5 or title 38, United States Code, as well as individuals whom the Department considers employees such as volunteers, without compensation employees, and students and other trainees.
- VA Contractors - VA contractors are all non-VA users having access to VA information resources through a contract, agreement, or other legal arrangement. Contractors must meet the security levels defined by the contract, agreement, or arrangement. Contractors must read and sign the Rules of Behavior and complete security awareness and privacy training prior to receiving access to the information systems.

Users agree to comply with all terms and conditions of the National Rules of Behavior by signing a certificate of training at the end of the training session.

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

If Yes, provide:

1. *The Security Plan Status,?*

   - a. *Approved*
2. *The Security Plan Status Date,*
   - a. *May 06, 2021*
3. *The Authorization Status,*
   - a. *Authorization to Operate (ATO)*
4. *TheS Authorization Date,*
   - a. *July 29, 2021*
5. *The Authorization Termination Date, .*
   - a. *Jan 17, 2023*
6. *The Risk Review Completion Date*
   - a. *July 12, 2021*
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH).*
   - a. *MODERATE*

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

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

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, 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.

This question is related to privacy control UL-1, Information Sharing with Third Parties.

AINS eCase -E does utilize Cloud technology based on the eCase platform. There is FedRAMP ATO for AINS – eCase. The full authorization package is available in OMB Max – the unique identifier is AGENCYHUDSAAS.

9.2 Identify the cloud model being utilized.

Example: Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Commercial off the Shelf (COTS).

This question is related to privacy control UL-1, Information Sharing with Third Parties.

Software as a Service (SaaS)

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

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

Yes. The contract number is VA118-16-D-1008 36C10B20N10080040.

9.4 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.

There is no ancillary data collected outside of the PII listed in section 1.1.

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

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

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

Yes. Specific language on data ownership and details around data management is detailed in section 5.6.1, 5.8.1, 5.11 and Part II Section 1, I.1 (FAR 52.227-14) of the contract (VA118-16-D-1008 36C10B20N10080040).

9.6 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).

RPA is not utilized within the AINS eCase product boundary.

Section 9. 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 provided in this Privacy Impact Assessment is true and accurate.

Jacquelyn R Filkins 190940

Digitally signed by Jacquelyn R Filkins 190940
Date: 2021.09.16 08:33:50 -04'00'

Privacy Officer, Jacquelyn Filkins

Karen A. McQuaid 321576

Digitally signed by Karen A. McQuaid 321576
Date: 2021.09.17 12:55:29 -05'00'

Information Security Systems Officer, Karen A. McQuaid

TRAVIS FRAYER

Digitally signed by TRAVIS FRAYER
Date: 2021.09.17 12:22:43 -04'00'

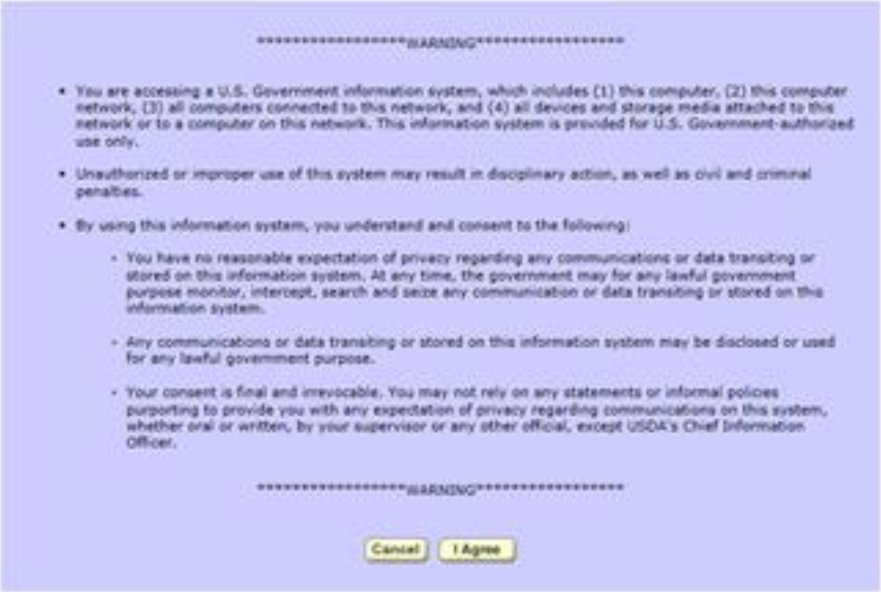
System Owner, Travis L. Frayer

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).

https://www.va.gov/privacy-policy/

Below is the privacy warning banner presented to VA user's before eCase logon:



******************WARNING******************

- You are accessing a U.S. Government information system, which includes (1) this computer, (2) this computer network, (3) all computers connected to this network, and (4) all devices and storage media attached to this network or to a computer on this network. This information system is provided for U.S. Government-authorized use only.
- Unauthorized or improper use of this system may result in disciplinary action, as well as civil and criminal penalties.
- By using this information system, you understand and consent to the following:
  - You have no reasonable expectation of privacy regarding any communications or data transiting or stored on this information system. At any time, the government may for any lawful government purpose monitor, intercept, search and seize any communication or data transiting or stored on this information system.
  - Any communications or data transiting or stored on this information system may be disclosed or used for any lawful government purpose.
  - Your consent is final and irrevocable. You may not rely on any statements or informal policies purporting to provide you with any expectation of privacy regarding communications on this system, whether oral or written, by your supervisor or any other official, except USDA's Chief Information Officer.

******************WARNING******************