The completion of Veterans Affairs Privacy Impact Assessments (PIAs) is mandated for any rulemaking, program, system, or practice that collects or uses PII under the authority of the E-government Act of 2002 (44 U.S.C. § 208(b)) and VA Directive 6508, Implementation of Privacy Threshold Analysis and Privacy Impact Assessment.

The PIA is designed to identify risk associated with the use of PII by a system, program, project or practice, and to ensure that vital data stewardship issues are addressed for all phases of the System Development Life Cycle (SDLC) of IT systems. It also ensures that privacy protections are built into an IT system during its development cycle. By regularly assessing privacy concerns during the development process, VA ensures that proponents of a program or technology have taken its potential privacy impact into account from the beginning. The PIA also serves to help identify what level of security risk is associated with a program or technology. In turn, this allows the Department to properly manage the security requirements under the Federal Information Security Management Act (FISMA).


Please note that the E-government Act of 2002 requires that a PIA be made available to the public. In order to comply with this requirement PIA will be published online for the general public to view. When completing this document please use simple, straight-forward language, avoid overly technical terminology, and write out acronyms the first time you use them to ensure that the document can be read and understood by the general public.
Privacy Impact Assessment for the VA IT System called:

Veterans Claim Intake Program
Records Management Service

(ACCUTRAC)

Date PIA submitted for review:
April 20, 2022

System Contacts:

<table>
<thead>
<tr>
<th>System Contacts</th>
<th>Name</th>
<th>E-mail</th>
<th>Phone Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy Officer</td>
<td>Jason L. Anderson</td>
<td><a href="mailto:Jason.Anderson3@va.gov">Jason.Anderson3@va.gov</a></td>
<td>(469) 927-8274</td>
</tr>
<tr>
<td>Information System Security Officer (ISSO)</td>
<td>Jose D. Diaz</td>
<td><a href="mailto:Jose.Diaz4@va.gov">Jose.Diaz4@va.gov</a></td>
<td>(312) 980-4215</td>
</tr>
<tr>
<td>Information System Owner</td>
<td>Derek L. Herbert</td>
<td><a href="mailto:Derek.Herbert@va.gov">Derek.Herbert@va.gov</a></td>
<td>(202) 461-9606</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>(202) 578-8084</td>
</tr>
</tbody>
</table>
Abstract

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

Iron Mountain’s ACCUTRAC® records management software application enables the VA to manage and have visibility of physical records, wherever they reside, from a single interface. ACCUTRAC provides a total records management solution for both on-site records and off-site records stored at Iron Mountain. The system allows the user to view inventory records and request retrieval of physical records from any Iron Mountain storage facility where the VA records are stored.

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?

ACCUTRAC® is owned by Iron Mountain Information Management, LLC. The software application is managed by an Iron Mountain internal Software Application Program Team and operated within an Iron Mountain data center facility at 1137 Branchton Road, Boyers, PA 16060. The ACCUTRAC instance deployed for the VA is a stand-alone instance that is not directly connected to any other source, or regional offices of GSS, VistA or LAN. This ACCUTRAC instance services the needs of the VA exclusively. ACCUTRAC receives all box and file data via data transfer via secure file transport (SFTP) supporting FIPS 140-2 encryption methods from the Intake Conversion and Mail Handling Services (ICMHS) vendor Systems Made Simple (SMS). The ACCUTRAC instance builds on Iron Mountain’s ironclad chain-of-custody and records management processes. No changes are required for existing Business Processes. The ACCUTRAC instance is being stood up with the latest hardware available in the marketplace and the software itself is Iron Mountain proprietary. No technology changes are foreseen for
the immediate future. Iron Mountain has an ISA/MOU in place with VA.

Through a partnership with Iron Mountain, The Department of Veterans Affairs (VA) continues to optimize the Veterans Benefits Management System (VBMS) to reduce the time required to establish, develop, decide, and pay claims. Iron Mountain’s relationship with the VBA has been built upon mutual success and synergies achieved through the Document Conversion Services (DCS) followed by the Intake Conversion and Mail Handling Services (ICMHS) Task Orders and through our performance under the current Record Management Services (RMS) contract. Iron Mountain continues to facilitate progress and efficiencies under the RMS contract as demands and requirements evolve through supply chain management, and operational leadership.

As noted above, Iron Mountain has provided the necessary support under DCS and ICMHS to consolidate records management services for previously converted claims related source material in order to support the VBA with efficient and accurate processing of Veterans disability claims. In an effort to provide the VBA with continued project support, Iron Mountain has worked to develop an effective computer-based inventory tracking system, that is PII compliant, allowing the VA to streamline the number of sources (outside of IM) used to identify the location/descriptors of a given file; this enhanced capability will better support the needs of the RMS contract. Iron Mountain has determined our ACCUTRAC® records management application will allow the VBA the best flexibility to effectively track all source material and maintain accurate status of all records in Iron Mountain’s facilities while meeting government security requirements for the ingestion and storage of PII metadata.

Iron Mountain’s ACCUTRAC software provides VBA with a simple interface used to track the status and location of VA shipments of physical claim files and other claims associated material. This system does not explicitly collect information about Veterans or beneficiaries; however, stores basic information related to the shipped/stored boxes and high-level details of the material that resides within. The information stored within the ACCUTRAC system does not contain information associated to VA benefits, it does not contain biometrics, Human Resource, or any other sensitive personal information, and does not produce, store, or present any Personally Identifiable Information (PII) other than a beneficiary’s name and VA file number (Social Security Number). The data that will be retained in the system consists of file and box metadata describing the contents of physical records stored at Iron Mountain facilities. Examples of the box/file metadata fields include but are not limited to:

- ICMHS Vendor ID (Example: “Leidos,” “SMS” or “SRA”)
- ICMHS Vendor-generated box identification number
- Date of transfer to RMS
- Records Management Number (RMN)
- Box Source (RMC, VARO, AMC, etc.)
- Veteran names associated with each box
- Veteran file numbers associated with each box
- Document Control Sheet (DCS) associated with each Veteran

The ACCUTRAC instance implemented for the VA is a stand-alone instance that houses all PII information. This instance extracts non-PII box level information from Iron Mountain’s SafeKeeper Plus inventory tracking system.

Iron Mountain is afforded the authority to be in receipt of this VA material and information in accordance with their contract with VA, specifically under the Task Order of GS-25F-0066M VA119-15-F-0123 dated July 14, 2017. This contract is operating under the appropriation number 101-3670151-5884-301700 Office of Business Proc-2580 Non-Medical Contracts and-020041000, requisition ID 101-17-2-5884-0024 (P). The official SORN for this material is listed under Notice of Amendment of System of
Records, “VA Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records—VA” (58VA21/22/28). The VA has conducted the necessary NSOC vulnerability scans and reviewed the full complement of IT documentation necessary to grant an Authority to Operate (ATO) which is active.

ACCUTRAC does not utilize any cloud components/solution/FedRAMP. No contracts are in place with Cloud Services providers and NIST 800-144 regulations do not apply.

This system is not the official system of record for this information. As with any system of record, or individual record, exposure of sensitive Veteran material is of consequence to the Veteran’s we serve, the VA and of course Iron Mountain. Our team holds this responsibility of data protection with the highest regard. The first measure of protection is always prevention and as such we have cleared personnel accessing the system, specific user roles with appropriate access that matches the “need to know.” Iron Mountain has developed, implemented, and demonstrated iron clad security disciplines to government and customer for decades. Should the unthinkable happen, Iron Mountain has established protocols that cover notification, escalation, comprehensive log reviews, breach arrest protocols and follow-through to complete resolution. Iron Mountain’s data breach protocols comply with the current Performance Work Statement (PWS).

The term “security incident” means an event that has, or could have, resulted in unauthorized access to or loss of VA assets or sensitive information, or an action that breaches VA security procedures. When a security incident occurs, the Contractor shall immediately notify the COR of any known or suspected security incidents or any unauthorized disclosure of sensitive information. The COR will provide specific instructions to address the incident.

Within 48 hours of a security incident, the Contractor shall provide to the COR a Security Incident Report, which shall address all relevant information concerning the security incident, including the following:

- Nature of the event (loss, theft, unauthorized access);
- Description of the event, including:
  - Date of occurrence.
  - Data elements involved, including any PII, such as full name, social security number, date of birth, home address, account number, disability code.
  - Number of individuals affected or potentially affected.
  - Names of individuals or groups affected or potentially affected.
  - Ease of logical data access to the lost, stolen or improperly accessed data in light of the degree of protection for the data, e.g., unencrypted, plain text.
  - Amount of time the data has been out of VA control.
  - The likelihood that the sensitive personal information will or has been compromised (made accessible to and usable by unauthorized persons).
  - Known misuses of data containing sensitive personal information, if any.
  - Assessment of the potential harm to the affected individuals.
  - Data breach analysis as outlined in 6500.2 Handbook, Management of Security and Privacy Incidents, as appropriate.
  - Whether credit protection services may assist record subjects in avoiding or mitigating the results of identity theft based on the sensitive personal information that may have been compromised.

The Iron Mountain facility where the duplicative physical material is stored is under strict physical security controls. The information system it subject to FISMA law and requires the Authority to Operate prior to handling and processing of VA sensitive information. The level of impact that could result from unauthorized disclosure of information, unauthorized modification of information,
unauthorized destruction of information, or loss of information or information system availability is set to an overall moderate level in accordance with NIST 800-37 and as defined by VBA system owner. The overall organizational risk to organizational operations (mission, functions, image, and reputation), organizational assets, individuals, other organizations, and/or the Nation are set to the moderate level.

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://www.va.gov/vapubs/). If the system creates information (for example, a score, analysis, or report), list the information the system is responsible for creating.

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

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

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

- Name
- Social Security Number
- Date of Birth
- Mother’s Maiden Name
- Personal Mailing Address
- Personal Phone Number(s)
- Personal Fax Number
- Personal Email Address
- Emergency Contact Information (Name, Phone Number, etc. of a different individual)
- Financial Account Information
- Health Insurance Beneficiary Numbers
- Account numbers
- Certificate/License numbers
- Vehicle License Plate Number
- Internet Protocol (IP) Address Numbers
- Current Medications
- Previous Medical Records
- Race/Ethnicity
- Tax Identification Number
- Medical Record Number
- Gender
- Integration Control Number (ICN)
- Military History/Service Connection
- Next of Kin
- Other Unique Identifying Information (list below)
The data identified above must be transferred to Iron Mountain from a VA identified vendor. Iron Mountain ACCUTRAC Software provides searchable metadata fields that enable the retrieval of physical records. VA personnel collect, upload and maintain the data that is entered into the metadata fields in ACCUTRAC.

**PII Mapping of Components**

ACCUTRAC consists of 2 key components. Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by ACCUTRAC and the reasons for the collection of the PII are in the table below.

**PII Mapped to Components**

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

<table>
<thead>
<tr>
<th>Database Name of the information system collecting/storing PII</th>
<th>Does this system collect PII? (Yes/No)</th>
<th>Does this system store PII? (Yes/No)</th>
<th>Type of PII (SSN, DOB, etc.)</th>
<th>Reason for Collection/Storage of PII</th>
<th>Safeguards</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACCUTRAC Database</td>
<td>Yes</td>
<td>Yes</td>
<td>Veteran Name, Veteran File Number (Social Security Number)</td>
<td>VBA Search &amp; Retrieve Needs</td>
<td>Database is encrypted and system is stored within a secure data center.</td>
</tr>
</tbody>
</table>

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.*
The data is supplied in a flat file, on a regular cadence, from VA contractors scanning Veteran material. The Task Orders involved are the Document Conversions Services (DCS), Intake Conversion and Mail Handling Services (ICMHS), Paper Mail Conversion and Management Services (PMCMS), File Bank Extraction (FBE) and Centralized Support Division (CSD). Data Version Date: February 27, 2020 Page 7 of 31 hosted on Iron Mountain’s ACCUTRAC system may be supplemented by specific VA users who want to append, or clarify, existing data records when a file retrieval/search is performed. Iron Mountain does not collect any information that is ingested into ACCUTRAC. The VA is the information owner. Iron Mountain receives the information from a VA supplied vendor via secure transfer and retains the information within ACCUTRAC for the purpose of physical record retrieval by a VA user.

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.

Information is transmitted using electronic transfer from a VA supplied vendor, the Iron Mountain ACCUTRAC system. The scanning conversion vendors operating under the Document Conversions Services (DCS), Intake Conversion and Mail Handling Services (ICMHS), Paper Mail Conversion and Management Services (PMCMS), File Bank Extraction (FBE) and Centralized Support Division (CSD). task orders transfer data via secure file transport (SFTP) supporting FIPS 140-2 encryption methods.

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.

Iron Mountain is not the information owner and receives all information from an authorized VA identified vendor. Iron Mountain will ingest information exactly as provided by the VA supplied vendor but is not responsible for accuracy of the transmitted information.
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

Iron Mountain is afforded the authority to be in receipt of this VA material and information under 38 U.S.C. § 5101(c)(1), serving as an Agent of the government, as well as in accordance with their contract with VA. Iron Mountain is afforded the authority to be in receipt of this VA material and information in accordance with their contract with VA, specifically under the Task Order of GS-03F-049GA 36C10D21F0004, dated November 28, 2020. This contract is operating under the appropriation number 101-3610151-5884-301700 Office of Business Proc-2580 Non-Medical Contracts and-020041000, requisition ID 101-21-1-5884-0007. The official SORN for this material is listed under Notice of Amendment of System of Records, “VA Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records--VA” (58VA21/22/28).

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

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

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

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

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

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

Principle of Data Quality and Integrity: Are there policies and procedures for VA to ensure that personally identifiable information is accurate, complete, and current?

This question is related to privacy control AR-1, Governance and Privacy Program, and AR-2, Privacy Impact and Risk Assessment.

Iron Mountain is responsible for the physical storage of VBA claims material that has been previously scanned and uploaded into the official System of Record, the Veterans Benefits Management System (VBMS) by another VA service vendor. By law, VBA cannot destroy these records therefore they must be maintained until disposition of these records is authorized through legislative action. The information Iron Mountain receives through its information system is provided by various VA approved vendors and is used to enable the retrieval and lookup of records within the Iron Mountain facility. The information
collected is the minimal information needed in order to locate these records with the only sensitive information being the Veteran’s file number. The Facility itself is subject to physical security controls outlined within the National Archives Records Administration (NARA) regulations. The NARA regulations affecting Federal agencies and their records management programs are found in Subchapter B of 36 Code of Federal Regulations Chapter XII. Iron Mountain has to obtain and maintain compliance with NARA regulations and is subject to audits if necessary, by VA authorities. As a part of the NARA requirements, strict physical security controls are in place both at the information system level and around the physical security of the physical material being stored within Iron Mountain’s secure storage facility.

Follow the format below when entering your risk assessment:

**Privacy Risk:** As a part of this contract, Iron Mountain maintains duplicative physical claims material as well as logical data within their information system. The information system, if compromised would expose limited VA sensitive information to the malicious actor in the form of Veteran Name and File Number. If the storage facility was compromised, the threat source and the execution of an event may have the potential to obtain access to said physical information which could violate the confidentiality of said information.

**Mitigation:** Iron Mountain implements strict environmental and technological security controls within both its information system and facilities to prevent the accidental exposure of VA sensitive information. Iron Mountain’s information system is undergoing the appropriate Assessment and Authorization (A&A) to obtain the Authority to Operate (ATO) from VA. Iron Mountain’s ACCUTRAC system is responsible for achieving the MODERATE security categorization in accordance with FIPS-199 to ensure confidentiality, integrity and availability of the information is maintained appropriately. All physical security controls area also subject of the A&A process as well as the duplicative physical material itself which is required to meet NARA compliance. All personnel with access to the information or the stored material have the appropriate level of background investigation and have received VA information security and privacy awareness training and signed the rules of behavior annually.

**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.*

Iron Mountain conducts a review of the data with the information owner / privacy officer (Agency) and conducts a review of the contractual agreements with Iron Mountain Legal Department to determine specific purpose for all PII that is stored/processed within the system. The PII data fields include:

- Veteran names associated with each box: used to identify and locate physical boxes and files for retrieval from Iron Mountain’s facilities for return to an authorized VA system user
- Veteran file numbers associated with each box (may be SSN): used to identify and locate physical boxes and files for retrieval from Iron Mountain’s facilities for return to an authorized VA system user
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.

The VA is the information owner and would be responsible for data analysis and production. Iron Mountain does not analyze or produce data.

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?

ACCUTRAC data is encrypted in transit using Transport Layer Security 1.2 (TLS 1.2) with an industry-standard AES-256 cipher. ACCUTRAC Application Data stored in the SQL Server Database is in encrypted at rest with AES-256.

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

Yes. Application user access is controlled by security access granted by VA administrators within the ACCUTRAC application. Only authorized users with need-to-know and the necessary permissions will be able to access records and perform functions.

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

In addition to data encryption and strong access controls, ACCUTRAC complies with the Federal Information Security Management ACT (FISMA) – Assessment & Authorization (A&A) activities. The ACCUTRAC application maintains an active Authorization to Operate (ATO). The systems hosting the ACCUTRAC application are located in an underground secure data center with strict physical, environmental, and access controls in place.

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

Users accessing Iron Mountain ACCUTRAC can only access the information they have been authorized to view, edit or share all other information, such as documents, files, folders, etc. are not visible to the user. All user privileges are restricted based on the document security assignments for functions such as updating metadata and adding annotation notes. This level of access controls significantly lowers the security risk for the entire system. Iron Mountain implements its cyber incident response process to validate the event, notify the agency and will work with the Agency to determine if a privacy breach has occurred. Users who violate VA security and privacy policies will have their access terminated immediately. All users of this system are required to have the appropriate level of background investigation as required by VA handbook 0710 and must annually take VA Information Security and Privacy awareness training and sign the VA National Rules of Behavior. Each user’s compliance with said trainings is managed by the local station and monitored as a part of VA’s CRISP compliance management. Iron Mountain is responsible for the security of the information maintained within their system and within their secure facilities.

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 data identified above must be transferred to Iron Mountain from a VA identified vendor. Iron Mountain ACCUTRAC Software provides searchable metadata fields that enable the retrieval of physical records. VA personnel collect, upload and maintain the data that is entered into the metadata fields in
ACCUTRAC. The data that will be retained in the system consists of file and box metadata describing the contents of physical records stored at Iron Mountain facilities. The PII box/file metadata fields include:

- Veterans names associated with each box
- Veteran file numbers associated with each box

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.

Iron Mountain retains and disposes of PII in accordance with the contractual agreement with the VA. Although disposition options are available to exercise within the contract, at this time VA does not have the legal authority to dispose of the duplicated paper material. We are currently storing it until further notice, pending rulings from the Office of General Council and legislative action. These records do not meet the definition of "Federal records" as defined in 44 U.S.C. 3301 and are therefore not bound to a NARA retention schedule found in §1234.32 Retention and disposition of electronic records.

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.

Iron Mountain retains and disposes of PII in accordance with the contractual agreement with the Agency. Currently, records are stored indefinitely. Optional task to limit storage period or dispose of records has not been issued. The storage facility meets NARA compliance to minimize threats to the information stored. These records do not meet the definition of "Federal records" as defined in 44 U.S.C. 3301 and are therefore not bound to a NARA retention schedule found in §1234.32 Retention and disposition of electronic records.

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

Iron Mountain retains and disposes of PII in accordance with the contractual agreement with the Agency. Currently, records are stored indefinitely. Optional task to limit storage period or dispose of records has not been issued. Upon completion of the contract, Iron Mountain will work with VA to remediate sensitive information. These records do not meet the definition of "Federal records" as defined in 44 U.S.C. 3301 and are therefore not bound to a NARA retention schedule found in §1234.32 Retention and disposition of electronic records. After the close of the contract, the vendor will provide VA with the data and the vendor will follow VA Handbook 6500.1 for electronic media sanitization procedures.

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.

Iron Mountain Policy prohibits the use of confidential data (PII) in development, testing or research environments. Information Classification and Handling (GSRS-5250) and Application Development (GSRS-5350).

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:** Prolonged retention of VA sensitive information creates the prolonged potential for the exercise of a threat event by any threat source. Currently, VA is under legal obligation to store records until further notice.

**Mitigation:** Currently, records are stored indefinitely with Iron Mountain. Optional task to limit storage period or dispose of records has not been issued. Currently, VA is under legal obligation to store records until further notice. Iron Mountain deploys strict security controls to prevent the exposure or unauthorized access to VA sensitive information by any unapproved third parties.

**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

<table>
<thead>
<tr>
<th>List the Program Office or IT System information is shared/received with</th>
<th>List the purpose of the information being shared/received with the specified program office or IT system</th>
<th>List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system</th>
<th>Describe the method of transmittal</th>
</tr>
</thead>
<tbody>
<tr>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

### 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:** N/A

**Mitigation:** N/A

### 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**

<table>
<thead>
<tr>
<th>List External Program Office or IT System information is shared/received with</th>
<th>List the purpose of information being shared / received / transmitted with the specified program office or IT system</th>
<th>List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program or IT system</th>
<th>List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)</th>
<th>List the method of transmission and the measures in place to secure data</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACCUTRAC</td>
<td>Iron Mountain</td>
<td>(ICMHS, FCS, PMCMS) Vendor ID, Vendor generated box identification number, Date of transfer to Records Management Services (RMS) facility, Records Management Number (RMN), Document Control Sheet (DCSID), Box Source, Veteran name, Veteran file number/Social Security Number</td>
<td>Secure Web User Interface (https)</td>
<td>ISA/MOU</td>
</tr>
<tr>
<td>DD Tracker</td>
<td>GCIO/Data Dimensions</td>
<td>(ICMHS, FCS, PMCMS) Vendor ID, Vendor generated box identification number, Date of transfer to Records</td>
<td>Data transfer via secure file</td>
<td>Performanc e Work Statement (PWS)</td>
</tr>
</tbody>
</table>
Management Services (RMS) facility, Records Management Number (RMN), Document Control Sheet (DCSID), Box Source, Veteran name, Veteran file number/Social Security Number

transport (SFTP) supporting FIPS 140-2 encryption methods

 Workflow Integration Engine (WIE)  Leidos/HLP  (ICMHS, FCS, PMCMS)  Vendor ID, Vendor generated box identification number, Date of transfer to Records Management Services (RMS) facility, Records Management Number (RMN), Document Control Sheet (DCSID), Box Source, Veteran name, Veteran file number/Social Security Number

Data transfer via secure file transport (SFTP) supporting FIPS 140-2 encryption methods

Performance Work Statement (PWS)

 Tracking Tool  Iron Mountain/GDI T  (ICMHS, FCS, PMCMS)  Vendor ID, Vendor generated box identification number, Date of transfer to Records Management Services (RMS) facility, Records Management Number (RMN), Document Control Sheet (DCSID), Box Source, Veteran name, Veteran file number/Social Security Number

Data transfer via secure file transport (SFTP) supporting FIPS 140-2 encryption methods

Performance Work Statement (PWS)

This Information System receives electronic inputs from the Intake Conversion and Mail Handling Services (ICMHS), the Paper Mail Conversion and Management Services (PMCMS), and the File Conversion Services (FCS) Information Systems via SFTP which provides Iron Mountain with the information found within the above table. The system does not store user inputs.

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

Discuss the privacy risks associated with the sharing of information outside the Department and what steps, if any, are currently being taken to mitigate those identified risks.

Discuss whether access controls have been implemented and whether audit logs are regularly reviewed to ensure appropriate sharing outside of the Department. For example, is there a Memorandum Of Understanding (MOU), contract, or agreement in place with outside agencies or foreign governments.

Discuss how the sharing of information outside of the Department is compatible with the stated purpose and use of the original collection.
This question is related to privacy control AR-2, Privacy Impact and Risk Assessment, AR-3, Privacy Requirements for Contractors and Service Providers, and AR-4, Privacy Monitoring and Auditing

Follow the format below:

**Privacy Risk:** There is a possibility of Unauthorized access to information.

**Mitigation:** Iron Mountain follows requirements outlined in its internal Information Classification and Handling Policy GSRS-5250 and in Access Control Policy GSRS-5150. Iron Mountain Access Control Policy is reviewed at least every 3 years or whenever there is a significant change. Iron Mountain Access Control procedures are reviewed at least annually. ACCUTRAC user accounts are granted access based on a business justification; membership to privileged groups is limited to users who require this level of access to perform their job function. For Iron Mountain corporate accounts, access is granted based on the least privilege approach and administrative access is restricted to those individuals who require such access to fulfill their job responsibilities. Administrative Access to the systems is limited in accordance with the Company Access Control Policy Global (GSRS-5150). Iron Mountain maintains metrics and reviews security logs to ensure compliance with the organization privacy policy and stated time frames. All personnel with access to Veteran’s information are required to complete the VA Privacy and Information Security Awareness training and Rules of Behavior annually.

In the event a Privacy complaint or incident is discovered, a Privacy, Security, Events and Tracking System (PSETS) ticket will be entered. PSETS is the tool VA uses for reporting and tracking a privacy event. You can request a PSETS account from an existing PSETS user or by contacting the PSETS Remedy Team. Be sure you know how to use PSETS because you’re required to report a privacy event within one hour of learning about it. By documenting a privacy event in PSETS, it serves as the central repository and authoritative data source concerning a privacy event. It also allows for prompt notification to your VA leadership and the DBRS.

Iron Mountain has developed an Incident Response Plan for the system that depicts the different phases of incident handling: preparation, detection and analysis, containment, eradication, and recovery. It also describes the breach notification process. All Iron Mountain employees are required to report incidents immediately. Iron Mountain has established a Cyber Incident Response Team (CIRT) that responds to and handles all cyber-related incidents and breaches.

**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.

Operating as an agent of VA, Iron Mountain operates under the Notice of Amendment of System of Records, VA Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records--VA" (58VA21/22/28) available at https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24372.pdf

Iron Mountain holds no direct responsibility for notice as it does not collect information from Veterans and is not the responsible information owner. Responsibility falls upon the VA Information Owner. The Veterans claims forms contain a Privacy Act Notice.

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

Any explicit opportunity and right to decline to provide information is managed by Department of Veterans Affairs (VA) under an existing system of records, “VA Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records—VA” (58VA21/22/28).

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

Any explicit opportunity and right to consent to a particular use of their information is managed by Department of Veterans Affairs (VA) under an existing system of records, “VA Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records—VA” (58VA21/22/28).

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:** Individuals might not be aware that their information is being collected.

**Mitigation:** Operating as an agent of VA, Iron Mountain operates under the Notice of Amendment of System of Records, "VA Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records--VA" (58VA21/22/28). The published SORN can be located at https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24372.pdf Iron Mountain holds no direct responsibility for notice as it does not collect information from Veterans and is not the responsible information owner. Responsibility falls upon the VA Information Owner and the Veterans Benefits Administration.

**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.

If an individual seeks compensation benefits records contained within a VA claims folder, or military service medical records in VA’s possession, the request will be fulfilled by the VA Claims Services Department as part of the Centralized FOIA/PA initiative. Requestors should mail or fax their Privacy Act or FOIA requests to the Intake Center in Janesville, Wisconsin: Department of Veterans Affairs Claims Intake Center P.O. Box 4444 Janesville, WI 53547-4444 Fax: 844-531-7818 DID: 608-373-6690.
If an individual seeks other benefits records maintained by VA, to include Vocational Rehabilitation & Employment, Insurance, Loan Guaranty or Education Service, you must submit these records to the FOIA/Privacy Act Officer at the VA Regional Office serving the individual's jurisdiction, or to the FOIA/Privacy Act Officer of the Veterans Benefits Administration, VA Central Office.

Additional information can be found on the VA privacy website: https://www.oprm.va.gov/foia/foia_howTo.aspx

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 information stored by Iron Mountain is not used for any claims related processes and is not the official system of record for VA. If the information within the system is incorrect, it does not provide any harm/risk to the individual as it is not shared with any external or internal shared party for record maintenance or claims development purposes. The VA is the information owner and would be responsible for correcting inaccurate or erroneous information.

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.

The information stored by Iron Mountain is not used for any claims related processes and is not the official system of record for VA. If the information within the system is incorrect, it does not provide any harm/risk to the individual as it is not shared with any external or internal shared party for record maintenance or claims development purposes. The VA is the information owner and would be responsible for correcting inaccurate or erroneous information.

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.
The information stored by Iron Mountain is not used for any claims related processes and is not the official system of record for VA. If the information within the system is incorrect, it does not provide any harm/risk to the individual as it is not shared with any external or internal shared party for record maintenance or claims development purposes. The VA is the information owner and would be responsible for correcting inaccurate or erroneous information.

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: There is a possibility that information is incorrect and the individual is unable to change their information.

Mitigation: The information stored by Iron Mountain is not used for any claims related processes and is not the official system of record for VA. If the information within the system is incorrect, it does not provide any harm/risk to the individual as it is not shared with any external or internal shared party for record maintenance or claims development purposes. The VA is the information owner and would be responsible for correcting inaccurate or erroneous information.

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.

Iron Mountain Access Control Policy Global (GSRS-5150) is implemented. The Policy includes sections and languages that provide clear descriptions of the Policy purpose, scope roles, responsibilities, management commitment, coordination among organizational entities and compliance. Iron Mountain will treat all data as if it contains PII and utilize Access controls within ACCUTRAC application to restrict access. Accounts related to ACCUTRAC are delegated to the agencies account approver roles. The ACCUTRAC end user accounts are delegated and managed by the federal agencies in ACCUTRAC. To efficiently manage user access permissions throughout ACCUTRAC environment, users are attached to access control groups, as appropriate, to control their access to information assets and network resources.

Iron Mountain Corporate Accounts are created for all Iron Mountain corporate users, contractors, and vendors where required. The Iron Mountain corporate network, which contains domain accounts for all IRM employees and vendors, is controlled and managed by group policy settings. All IRM employees, contractors and vendors have an account that provides access to the corporate network to access basic corporate resources like email, network, file servers, and SharePoint etc. Iron Mountain has two major account types: Staff Accounts and Service Accounts. Staff Accounts are IRM domain user accounts assigned to Operations personnel, contractors and vendors responsible for the implementation and operation of IRM SOFTWARE hosted infrastructure or Hosted Services. Service accounts may be used to execute service components such as IIS, SQL, backup and batch jobs etc. Access to the in-scope systems is granted based on least privilege and administrative access is restricted to those individuals who require such access to fulfill their job responsibilities. Administrative access to the systems is limited in accordance with the Iron Mountain Access Control policies and the ACCUTRAC Access Control Standard Operating Procedure (AC SOP).

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.
ACCUTRAC is owned and maintained by Iron Mountain. Access to the in-scope systems and PII is granted based on least privilege and administrative access is restricted to those individuals who require such access to fulfill their job responsibilities. Administrative access to the systems is limited in accordance with the Iron Mountain Access Control policies. All Iron Mountain users with access to the VA data complete an appropriate background investigation for their role, sign a confidentiality agreement, and complete VA and Iron Mountain required Privacy Training.

The Office of Business Integration (OBI) will be providing Iron Mountain with a list of authorized users.

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.

Iron Mountain has developed a training and awareness strategy in accordance to organizational policy. The strategy includes annual privacy and security training, posting on corporate intranet, screen saver messages and by using other internal communication mechanisms such as team and department meetings. Personnel directly responsible for dealing with PII go through additional annual training that includes online training. Personnel upon completion of their annual training are required to acknowledge they have read the appropriate policies and understand their responsibilities under those policies.

All individuals that interact with the VA ACCUTRAC are also subject to the annual VA Privacy Training module that is offered through the VA’s Talent management System (TMS).

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

If Yes, provide:

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

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

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

The Authorization to Operate (ATO) for the ACCUTRAC Application was granted on January 10, 2022. The ATO is valid for one year and expires on January 10, 2023. The Security Plan is active and up to date.
with an approved status date of February 3, 2022. The FIPS 199 classification of the system is MODERATE. An RMF Risk Assessment Report was developed and signed off by the VA System Owner and Information Security Officer on November 1, 2021.

**Section 9 – Technology Usage**

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

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

*If so, Does the system have a FedRAMP provisional or agency authorization? If the system does use cloud technology, but does not have FedRAMP authorization, explain how the Cloud Service Provider (CSP) solution was assessed and what FedRAMP documents and processes were used for the assessment in order to comply with VA Handbook 6517. Types of cloud models include Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Commercial off the Shelf (COTS).*

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

*Note: For systems utilizing the VA Enterprise Cloud (VAEC), no further responses are required after 9.1.*

The ACCUTRAC application does not utilize cloud technologies.

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

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

The ACCUTRAC application does not utilize cloud technologies.

**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 ACCUTRAC application does not utilize cloud technologies.

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

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

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

The ACCUTRAC application does not utilize cloud technologies.

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 ACCUTRAC application does not utilize cloud technologies.
### Section 10. References

**Summary of Privacy Controls by Family**

<table>
<thead>
<tr>
<th>ID</th>
<th>Privacy Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>AP</td>
<td>Authority and Purpose</td>
</tr>
<tr>
<td>AP-1</td>
<td>Authority to Collect</td>
</tr>
<tr>
<td>AP-2</td>
<td>Purpose Specification</td>
</tr>
<tr>
<td>AR</td>
<td>Accountability, Audit, and Risk Management</td>
</tr>
<tr>
<td>AR-1</td>
<td>Governance and Privacy Program</td>
</tr>
<tr>
<td>AR-2</td>
<td>Privacy Impact and Risk Assessment</td>
</tr>
<tr>
<td>AR-3</td>
<td>Privacy Requirements for Contractors and Service Providers</td>
</tr>
<tr>
<td>AR-4</td>
<td>Privacy Monitoring and Auditing</td>
</tr>
<tr>
<td>AR-5</td>
<td>Privacy Awareness and Training</td>
</tr>
<tr>
<td>AR-7</td>
<td>Privacy-Enhanced System Design and Development</td>
</tr>
<tr>
<td>AR-8</td>
<td>Accounting of Disclosures</td>
</tr>
<tr>
<td>DI</td>
<td>Data Quality and Integrity</td>
</tr>
<tr>
<td>DI-1</td>
<td>Data Quality</td>
</tr>
<tr>
<td>DI-2</td>
<td>Data Integrity and Data Integrity Board</td>
</tr>
<tr>
<td>DM</td>
<td>Data Minimization and Retention</td>
</tr>
<tr>
<td>DM-1</td>
<td>Minimization of Personally Identifiable Information</td>
</tr>
<tr>
<td>DM-2</td>
<td>Data Retention and Disposal</td>
</tr>
<tr>
<td>DM-3</td>
<td>Minimization of PII Used in Testing, Training, and Research</td>
</tr>
<tr>
<td>IP</td>
<td>Individual Participation and Redress</td>
</tr>
<tr>
<td>IP-1</td>
<td>Consent</td>
</tr>
<tr>
<td>IP-2</td>
<td>Individual Access</td>
</tr>
<tr>
<td>IP-3</td>
<td>Redress</td>
</tr>
<tr>
<td>IP-4</td>
<td>Complaint Management</td>
</tr>
<tr>
<td>SE</td>
<td>Security</td>
</tr>
<tr>
<td>SE-1</td>
<td>Inventory of Personally Identifiable Information</td>
</tr>
<tr>
<td>SE-2</td>
<td>Privacy Incident Response</td>
</tr>
<tr>
<td>TR</td>
<td>Transparency</td>
</tr>
<tr>
<td>TR-1</td>
<td>Privacy Notice</td>
</tr>
<tr>
<td>TR-2</td>
<td>System of Records Notices and Privacy Act Statements</td>
</tr>
<tr>
<td>TR-3</td>
<td>Dissemination of Privacy Program Information</td>
</tr>
<tr>
<td>UL</td>
<td>Use Limitation</td>
</tr>
<tr>
<td>ID</td>
<td>Privacy Controls</td>
</tr>
<tr>
<td>------</td>
<td>---------------------------------------</td>
</tr>
<tr>
<td>UL-1</td>
<td>Internal Use</td>
</tr>
<tr>
<td>UL-2</td>
<td>Information Sharing with Third Parties</td>
</tr>
</tbody>
</table>
Signature of Responsible Officials

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

JASON L. ANDERSON 509044
Digitally signed by JASON L. ANDERSON 509044
Date: 2022.04.28 07:42:56 -04'00'

Privacy Officer, Jason L. Anderson

Jose Diaz 386249
Digitally signed by Jose Diaz 386249
Date: 2022.04.28 08:42:47 -05'00'

Information Systems Security Officer, Jose D. Diaz

DEREK HERBERT
Digitally signed by DEREK HERBERT
Date: 2022.04.28 09:14:13 -04'00'

Information System Owner, Derek L. Herbert
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).

PRIVACY ACT NOTICE: The form will be used to determine allowance to compensation benefits (38 U.S.C. 5101). The responses you submit are considered confidential (38 U.S.C. 5701). VA may disclose the information that you provide, including Social Security numbers, outside VA if the disclosure is authorized under the Privacy Act, including the routine uses identified in the VA system of records, 58VA21/22/28, Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records – VA, published in the Federal Register. The requested information is considered relevant and necessary to determine maximum benefits under the law. Information submitted is subject to verification through computer matching programs with other agencies. VA may make a “routine use” disclosure for: civil or criminal law enforcement, congressional communications, epidemiological or research studies, the collection of money owed to the United States, litigation in which the United States is a party or has an interest, the administration of VA programs and delivery of VA benefits, verification of identity and status, and personnel administration. Your obligation to respond is required in order to obtain or retain benefits. Information that you furnish may be utilized in computer matching programs with other Federal or State agencies for the purpose of determining your eligibility to receive VA benefits, as well as to collect any amount owed to the United States by virtue of your participation in any benefit program administered by the Department of Veterans Affairs. Social Security information: You are required to provide the Social Security number requested under 38 U.S.C. 5101©(1). VA may disclose Social Security numbers as authorized under the Privacy Act, and, specifically may disclose them for purposes stated above.