Privacy Impact Assessment for the VA IT System called:

Veterans Claim Intake Program Records Management Service Assessing

Veterans Business Administration (VBA)

eMASS ID #186

Date PIA submitted for review:

February 05, 2024

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Marvis Harvey	Marvis.harvey@va.gov	202-461-8401
Information System Security Officer (ISSO)	Jose D. Diaz	jose.diaz4@va.gov	312-980-4215
Information System Owner	John D. Clark	john.clark7@va.gov	708-830-3616

Abstract

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

1 General Description

A. What is the IT system name and the name of the program office that owns the IT system?

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 VBA exclusively.

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

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. 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.

C. Who is the owner or control of the IT system or project?

The ACCUTRAC software instance itself is Iron Mountain proprietary.

2. Information Collection and Sharing

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

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 of over 12.6 million veterans. ACCUTRAC does not produce, store, or present any Personally Identifiable Information (PII) other than a beneficiary's VA name and file number (Social Security Number). The information stored within the ACCUTRAC system does not contain information associated to VA benefits, and it does not contain biometrics. The data that is retained in the system consists of file and box metadata describing the contents of physical records stored at Iron Mountain facilities.

E. What is a general description of the information in the IT system and the purpose for collecting this information?

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. 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

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

No information sharing is done. Only the VBA and Iron Mountain have access to ACCUTRAC.

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

The ACCUTRAC system is only operated out of one site (Iron Mountain, Boyers, PA Facility).

3. Legal Authority and SORN

H. What is the citation of the legal authority to operate the IT system?

Iron Mountain is afforded the authority to be in receipt of this VA material and information in according 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).

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

ACCUTRAC does not utilize any cloud components/solution/FedRAMP. No contracts are in place with Cloud Services providers and NIST 800-1444 regulations do not apply.

4. System Changes

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

No

K. Will the completion of this PIA could potentially result in technology changes?
No

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?

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

- ☒ Name
- ☒ Social Security Number
- ☐ Date of Birth
- ☐ Mother's Maiden Name
- ☐ Personal Mailing Address
- ☐ Personal Phone Number(s)
- ☐ Personal Fax Number
- ☐ Personal Email Address
- ☐ Emergency Contact Information (Name, Phone Number, etc. of a different individual)
- ☐ Financial Information
- ☐ Health Insurance Beneficiary Numbers Account numbers
- ☐ Certificate/License numbers[1]
- ☐ Vehicle License Plate Number
- ☐ Internet Protocol (IP) Address Numbers
- ☐ Medications
- ☐ Medical Records
- ☐ Race/Ethnicity
- ☐ Tax Identification Number
- ☐ Medical Record Number
- ☐ Gender
- ☐ Integrated Control Number (ICN)
- ☐ Military History/Service Connection
- ☐ Next of Kin
- ☐ Other Data Elements (list below)

PII Mapping of Components (Servers/Database)

ACCUTRAC consists of 1 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.

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

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

Internal Components Table

Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI	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
ACCUTRAC Database	Yes	Yes	- Veteran's Name - Veteran's File Number (Social Security Number)	VBA Search & Retrieve Needs	Database is encrypted and system is stored within a secure data center.

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

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

The 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.

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

Iron Mountain does not collect any information that is ingested into ACCUTRAC. The VA is the information owner. Iron Mountain receives the information from the VA web application and retains the information within ACCUTRAC for the purpose of physical record retrieval by a VA user.

1.2c Does the system create information (for example, a score, analysis, or report), list the system as a source of information?

Iron Mountain does not create any information that is ingested into ACCUTRAC. The VA is the information owner. Iron Mountain receives the information from the VA web application and retains the information within ACCUTRAC for the purpose of physical record retrieval by a VA user.

1.3 How is the information collected?

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

Information is collected by downloading the data from a VA web application, then imported into Iron Mountain ACCUTRAC system.

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

Information is collected by downloading the data from a VA web application, not on a form.

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

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

Iron Mountain is not the information owner and receives all information from an authorized VA identified vendor. The VA supplied vendor is responsible for ensuring the data us not corrupted.

1.4b Does the system check for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract?

No, Iron Mountain ingest the 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 according 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

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 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 must 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.

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's Name and File Number (Social Security). 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 that will be used in support of the program's business purpose.

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 Name and File Number (Social Security).

PII/PHI Data Element	Internal Use	External Use
Veteran's 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	Not used
Veteran's 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	Not used

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

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

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

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

The 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.

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information.

2.4a How is access to the PII determined?

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.

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

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.

2.4c Does access require manager approval?

Yes

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

Yes

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

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?

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?

Iron Mountain retains and disposes of PII in accordance with the contractual agreement with the VA. The source materials and data stored by the Contractor until the end of the Period of Performance. At this time, the transition of data shall encompass two (2) phases. The historical data through 180 calendar days prior to the expiration of the final period of performance shall be transitioned in phase 1. During phase 2 the remaining data from 180 calendar days prior to contract expiration through closeout shall be transitioned.

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)?

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

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.

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

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.

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

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?

Iron Mountain Policy prohibits the use of confidential data (PII) in development, testing or research environments.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

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?

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system***	***Describe the method of transmittal***
Veterans Benefits Administration (VBA)	ACCUTRAC software provides Veterans Benefits Administration (VBA) with a simple interface used to track the status and location of VA shipments of physical claim files and other claims associated.	Veteran's name, Veteran's file number/Social Security Number	Secure Web User Interface (https)

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

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

Mitigation: Iron Mountain follows requirements outlined in its internal ACCUTRAC Access Control (AC) Policy and Procedures. Iron Mountain Access Control Policy is reviewed at least every 5 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 ACCUTRAC Access Control (AC) Policy and Procedures. 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 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.

Data Shared with External Organizations

List External Program Office or IT System information is shared/received with	***List the purpose of information being shared / received / transmitted with the specified***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted)with the Program or IT system***	***List the legal authority, binding agreement, SORN routine use, etc. that permit***	***List the method of transmission and the measures in place to secure data***

	program office or IT system		***external sharing (can be more than one)***	
N/A	N/A	N/A	N/A	N/A

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

Privacy Risk: There is a low risk. There is a possibility that Iron Mountain/VA could inappropriately use or disclose information, either intentionally or unintentionally.

Mitigation: The ACCUTRAC web application site cannot be accessed from any external organization and/or site outside of the VA network. Only authorized VA users can access the site through the use of Single Sign On (SSOi) while on the VA network. Also, Iron Mountain follows requirements outlined in its internal ACCUTRAC Access Control (AC) Policy and Procedures. 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 ACCUTRAC Access Control (AC) Policy and Procedures.
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.

Section 6. Notice

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

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

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

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

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

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?

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?

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

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?

7.1a Cite any procedures or regulations your program has in place that allow access to information. These procedures, at a minimum, should include the agency's FOIA/Privacy Act practices, but may also include additional access provisions.

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

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

ACCUTRAC is not exempt from the access provisions of the Privacy Act

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

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?

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?

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?

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

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?

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

Iron Mountain ACCUTRAC Access Control Policy/SOP 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. 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. 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.

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

No users outside of the authorized Iron Mountain and VA users are allowed access to the ACCUTRAC system.

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

Iron Mountain privileged users have administrative rights for system maintenance/troubleshooting. On the application, authorized VA users have read-only rights. Service accounts may be used to execute service components such as Internet Information Services (IIS), Structured Query Language (SQL), backup, and batch jobs etc.

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?

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?

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?

8.4a If Yes, provide:

1. *The Security Plan Status:* Active
2. *The System Security Plan Status Date:* January 25, 2024
3. *The Authorization Status:* Valid
4. *The Authorization Date:* October 23, 2023
5. *The Authorization Termination Date:* April 20, 2024
6. *The Risk Review Completion Date:* January 25, 2024
7. *The FIPS 199 classification of the system:* Moderate

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?

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).

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?

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?

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.

The ACCUTRAC application does not utilize cloud technologies.

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

Signature of Responsible Officials

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

MARVIS HARVEY Digitally signed by MARVIS HARVEY
Date: 2024.02.09 13:35:42 -06'00'

Privacy Officer, Marvis Harvey

JOSE DIAZ Digitally signed by JOSE DIAZ
Date: 2024.02.12 14:42:46 -06'00'

Information System Security Officer, Jose D. Diaz

JOHN CLARK Digitally signed by JOHN CLARK
Date: 2024.02.09 16:53:13 -06'00'

Information System Owner, John D. Clark

APPENDIX A-6.1

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. Privacy, Policies, And Legal Information | Veterans Affairs

HELPFUL LINKS:

General Records Schedule
https://www.archives.gov/records-mgmt/grs.html

National Archives (Federal Records Management):
https://www.archives.gov/records-mgmt/grs

VA Publications:
https://www.va.gov/vapubs/

VA Privacy Service Privacy Hub:
https://dvagov.sharepoint.com/sites/OITPrivacyHub

Notice of Privacy Practice (NOPP):
VHA Notice of Privacy Practices
VHA Handbook 1605.04: Notice of Privacy Practices