Privacy Impact Assessment for the VA IT System called:

Resolution Management System Infrastructure (RMSI)

VA Office of Information and Technology (OIT)

Office of Resolution Management, Diversity & Inclusion (ORMDI)

eMASS ID 949

Date PIA submitted for review:

December 06, 2023

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Zulema Bolivar	Zulema.Bolivar@va.gov	202-461-6932
Information System Security Officer (ISSO)	Anthony McFarlane	Anthony.McFarlane2@va.gov	720-827-5438
Information System Owner	Glenn Thomas	Glenn.Thomas@va.gov	202-461-0293

Abstract

The abstract provides the simplest explanation for "what does the system do?".

The Resolution Management System Infrastructure (RMSI) is an enterprise-wide system that includes infrastructure and servers that will be housed on the VA Enterprise Cloud Services "Microsoft Azure hosted platform." The system contains one application: Complaints Automated Tracking System (CATS) and the ORMDI system users file server. CATS was a mission-critical system necessary for the conduct of the Office of Resolution Management's (ORMDI) day-to-day operations but is being phased out with the standup of the Equal Employment Opportunity EcoSystem (EEOE) designated as "E^2".

Overview

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

1 General Description

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

Resolution Management Systems Infrastructure (RMSI) / Office of Resolution Management, Diversity & Inclusion (ORMDI).

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

The Deputy Assistant Secretary for Resolution Management, Diversity & Inclusion (DAS/RMDI) has been delegated authority to supervise and control the operation of the administrative equal employment opportunity (EEO) discrimination complaint processing system within the whole of VA. The DAS/RMDI exercises exclusive authority to establish and modify discrimination complaint processing procedures. In pursuit of these objectives, the Complaints Automated Tracking System (CATS) gives the VA's Office of Resolution Management, Diversity & Inclusion (ORMDI) the ability to perform their mission.

ORMDI promotes a healthy working environment through prevention, resolution, and the processing of workplace disputes, including complaints of discrimination. ORMDI, with a staff of more than 330 people across the country, processes more than 5,000 EEO complaints for the Department of Veterans Affairs (VA) each year. CATS was the main repository of essential documents in the equal employment opportunity (EEO) process, however ORMDI has moved all new case entry to the Equal Employment Opportunity EcoSystem (EEOE), designated as E^2. CATS is being phased out but still currently assists ORMDI in its objectives to promote a healthy working environment through the prevention, resolution, and processing of workplace disputes, including complaints of

discrimination. CATS also enables ORMDI to meet the statutory deadlines for processing and adjudicating EEO complaints and monitoring settlement agreements.

RMSI includes infrastructure and servers that are housed on the VA Enterprise Cloud Services "Microsoft Azure-hosted platform." The system contains one application: Complaints Automated Tracking System (CATS) and the ORMDI File Server. This system, the application that it supports and the ORMDI File Server are necessary to the conduct of the Office of Resolution Management's (ORMDI) day-to-day operations.

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

VA Owned and VA Operated Information System

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?

- There are approximately 32,821 cases in CATS. Each case can have one or many Aggrieved Parties and many contacts and Counselors or Supervisors also associated.
- CATS contains essential documents for the Equal Employment Opportunity (EEO) process. Employees make complaints via government email, government phone lines, verbally to their supervisor or through a representative. Complainant information is entered into the application, which are then managed in the CATS application with email notifications, document (letter) templates, a shared document repository, and common reporting architecture.

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

- General Description of Information: CATS is the main repository of essential documents in the EEO complaint process: EEO Complaints Informal and Formal, Conflict Resolutions (CR) and Settlement Agreements: Aggrieved Parties, Complaint, legal documents, statement of witnesses, reports of interviews, records of investigations, fact finding reports, recommendations, final decisions, request for reconsideration and reconsideration decisions, contact information and case details.
- Purpose for Collecting Information: An employee, former employee, or applicant for employment, who believes discrimination occurred on the bases of race, color, religion, sex, sexual orientation, transgender orientation, national origin, age (40 or over), disability, genetic information, or retaliation for EEO activities, may initiate a complaint of discrimination. Once a written complaint is received, it will be reviewed for procedural sufficiency and then referred to the primary Administration (Veterans Health Administration, Veterans Benefits Administration or National Cemetery Administration) for further processing, including the investigative process (which will address those issues that were raised in the complaint) and the findings or resolution of those issues involved.

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

CATS Case and Contact Information is provided to other Internal VA Entities to effect notifications as listed below:

Internal System Name	Data Direction & Information	Type of Connection	Agreements Established
Veterans Benefits Administration (VBA)/email	Bidirectional Contact information, case details	Internal VA	N/A
Veterans Health Administration (VHA)/email	Bidirectional Contact information, case details	Internal VA	N/A
The Department of Veterans Affairs Central Office (VACO)/email	Bidirectional Contact information, case details	Internal VA	N/A
National Cemetery Administration (NCA)/email	Bidirectional Contact information, case details	Internal VA	N/A
Office of Information Technology	Bidirectional Contact Information, case details	Internal VA	N/A
VA Office of General Counsel	Unidirectional from CATS to OGC	Internal VA	N/A

ORMDI's EEO operational staff around the country have access to CATS. VA's Office of Employment Discrimination Complaint Adjudication in Washington, DC has limited, read-only access to CATS as well as permission to attach documents to a designated folder.

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?

RMSI includes infrastructure and servers that are housed on the VA Enterprise Cloud Services "Microsoft Azure Government Cloud hosted platform." Hosting occurs at a Primary and Alternate site with direct connections to the VA TIC (Trusted Internet Connection) from each location. PII is maintained consistently at both sites and all controls are used across both sites. CATS is an internal system to be used enterprise wide across the Department of Veteran Affairs three administrations.

3. Legal Authority and SORN

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

- 42 U.S.C. 2000e-16(b) and (c) Employment by Federal Government:
  - (b) Equal Employment Opportunity Commission; enforcement powers; issuance of rules, regulations, etc.; annual review and approval of national and regional equal employment opportunity plans; review and evaluation of equal employment opportunity programs and publication of progress reports; consultations with interested parties; compliance with rules, regulations, etc.; contents of national and regional equal employment opportunity plans; authority of Librarian of Congress; and,
  - (c) Civil action by employee or applicant for employment for redress of grievances; time for bringing of action; head of department, agency, or unit as defendant
- 29 U.S.C. 204 (f)-Establish Wage and Hour Division under the DoL
- 29 U.S.C. 206(d)-Prohibition of sex discrimination
- 29 U.S.C. 633(a)-Non-discrimination on account of age in Federal Government employment
- 29 U.S.C. 791 – Employment of individuals with disabilities
- Reorganization Plan No. 1 of 1978 – Federal Equal Employment Opportunity Activities
- 42 FR 69 (January 3, 1977) – Federal Register Notice
- 43 FR 19607 (May 9, 1978) – Federal Register Notice Appendix B – Additional Routine Uses for Systems EEOC-2 and 4-13
- Executive Order No. 11478 – Equal Employment Opportunity in the Federal Government
  - Amended by Executive Order 12106 (12/28/1978) and 44 FR 1053 (Jan. 3, 1979)– Transfer of certain equal employment enforcement functions
- The System of Record (SORN) 203VA08/87 FR 31058 –Diversity and Equal Employment Opportunity (EEO) Program Records – VA, Department of Veterans Affairs (VA), Office of Resolution Management, Diversity and Inclusion (ORMDI) – published 5/20/2022 - 2022-10848.pdf (govinfo.gov).

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?

Records compiled in CATS comprise the 203VA08/87 FR 31058 System of Records. The SORN notes records are maintained in file folders and electronically as published in the Federal Register. No change to the SORN is needed.

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?

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

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

The information selected below must match the information provided in question 2.1 as well as the data elements columns in 4.1 and 5.1. It must also match the information provided in question 3.4 of the PTA.

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)

Other PII/PHI data elements: Year of birth, Memos, letters and emails, Affidavits, Legal documents, Correspondence, and other documents pertinent to the EEO Employment Complaint

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

(e.g., employment data, applications for employment, disciplinary actions, etc.), Settlement Agreements.

PII Mapping of Components (Servers/Database)

RMSI consists of key components (servers/databases/instances/applications/software/application programming interfaces (API). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by RMSI 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. The first table of 3.9 in the PTA should be used to answer this question.

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
CATS File Server	Y	N	Name, Personal Mailing Address, Personal Phone Number(s), Personal Fax Number, Personal Email Address, Race/Ethnicity, Year of birth, Memos, letters and emails, Affidavits, Legal documents, Correspondence and other documents pertinent to the EEO Employment Complaint (e.g., employment data, applications for employment, disciplinary actions, etc.), Settlement Agreements	EEO Case Adjudication	Data is encrypted in transit and at rest. Access to the system is limited; access is audit

CATS Database Instance	Y	N	Name, Personal Mailing Address, Personal Phone Number(s), Personal Fax Number, Personal Email Address, Race/Ethnicity, Year of birth, Memos, letters and emails, Affidavits, Legal documents, Correspondence and other documents pertinent to the EEO Employment Complaint (e.g., employment data, applications for employment, disciplinary actions, etc.), Settlement Agreements	EEO Case Adjudication	Data is encrypted in transit and at rest. Access to the system is limited; access is audit
ORMDI File Server	Y	N	Name, Personal Mailing Address, Personal Phone Number(s), Personal Fax Number, Personal Email Address, Race/Ethnicity, Year of birth, Memos, letters, and emails, Affidavits, Legal documents, Correspondence and other documents pertinent to the EEO Employment Complaint (e.g., employment data, applications for employment, disciplinary actions, etc.),	EEO Case Adjudication	Data is encrypted in transit and at rest. Access to the system is limited; access is audit

			Settlement Agreements		
ORMDI Data Science Instance	Y	N	Name, Personal Mailing Address, Personal Phone Number(s), Personal Fax Number, Personal Email Address, Race/Ethnicity, Year of birth, Memos, letters and emails, Affidavits, Legal documents, Correspondence and other documents pertinent to the EEO Employment Complaint (e.g., employment data, applications for employment, disciplinary actions, etc.), Settlement Agreements	EEO Case Adjudication	Data is encrypted in transit and at rest. Access to the system is limited; access is audit

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

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

All initial case information is collected directly from the individual: Aggrieved Party, Complainant (VA Form 4939 (OMB Control Number: 2900-0716)), Employee, Witness, Legal Representatives, or Veteran.

Supportive information is provided by the following:

- Veterans Benefits Administration (VBA) – Compiling personal information
- Veterans Health Administration (VHA) – Compiling personal information
- National Cemetery Administration (NCA) – Compiling personal information
- The Department of Veterans Affairs Central Office (VACO) – Compiling personal information
- The Office of Information Technology – Compiling personal information

- Personnel-related information from HR

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.

Information comes from the Aggrieved Party (Individual), witnesses and OGC/EEOC using the following sources:

•EEO complaint form (4939)
• Memos, letters, and emails
• Affidavits
• Settlement agreements
• Legal documents (final agency decisions and actions)
• Correspondence and other documents pertinent to the EEO complaint, e.g., employment data, applications for employment, disciplinary actions, etc.

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

- Complaint Form 4939
- Affidavits and legal documents (final agency decisions and actions)
- System record resolution rates
- Processing time
- Savings reports
- Offer rates
- Case closure/performance metrics
- Settlement Report metrics
- Basis of Complaints
- EEO Complaint Data by type, formal/informal, location and by individuals
- Participation rates, and other EEOC data
- Emails with Notice Forms as required by law
- Congressional, Presidential, and EEOC Reporting

(No Personal data is aggregated in these reports)

1.3 How is the information collected?

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

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

- Information is collected directly from the complainant and witnesses.

- VA Form 4939 (OMB Control Number: 2900-0716) – During or shortly after the interactive discussion with the employee, authorized users will access CATS and complete necessary portions of the request
- Information collected directly from the employee via face to face, email, phone call and or third party
- Personnel-related information from HR
- Veterans Benefits Administration (VBA) – Compiling personal information via email
- Veterans Health Administration (VHA) – Compiling personal information via email
- National Cemetery Administration (NCA) – Compiling personal information via email
- The Department of Veterans Affairs Central Office (VACO) – Compiling personal information vis email
- The Office of Information Technology – Compiling personal information via email

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?

VA Form 4939 (OMB Control Number: 2900-0716)

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

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

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

Information in CATS is supplied by:

- The complainant – the complainant is responsible for ensuring its accuracy.
- Personnel records supplied by the HR office – the HR manager certifies its accuracy.
- Direct testimony from witnesses that is reviewed and signed by the witnesses.
- In addition, information collected from CATS is checked by the individual who entered the information in CATS.

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?

There is no third-party system check as the person provides the needed information to process the request as required by law.

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

- 42 U.S.C. 2000e-16(b) and (c) Employment by Federal Government:
  (b) Equal Employment Opportunity Commission; enforcement powers; issuance of rules, regulations, etc.; annual review and approval of national and regional equal employment opportunity plans; review and evaluation of equal employment opportunity programs and publication of progress reports; consultations with interested parties; compliance with rules, regulations, etc.; contents of national and regional equal employment opportunity plans; authority of Librarian of Congress; and,
  (c) Civil action by employee or applicant for employment for redress of grievances; time for bringing of action; head of department, agency, or unit as defendant
- 29 U.S.C. 206(d)-Prohibition of sex discrimination
- 29 U.S.C. 633(a)-Non-discrimination on account of age in Federal Government employment
- 29 U.S.C. 791 – Employment of individuals with disabilities
- Reorganization Plan No. 1 of 1978 – Federal Equal Employment Opportunity Activities
- 42 FR 69 (January 3, 1977) – Federal Register Notice
- 43 FR 19607 (May 9, 1978) – Federal Register Notice Appendix B – Additional Routine Uses for Systems EEOC-2 and 4-13
- Executive Order No. 11478 – Equal Employment Opportunity in the Federal Government
  - Amended by Executive Order 12106 (12/28/1978) and 44 FR 1053 (Jan. 3, 1979)– Transfer of certain equal employment enforcement functions.

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

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

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

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

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

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

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

Follow the format below when entering your risk assessment:

Privacy Risk:

1. Risk of people with no need to know accessing the information.
2. Risk of people not relinquishing access privileges when they should.

Mitigation:

1. Access Controls: The universe of individuals permitted to view case information is rigidly controlled by the system administrators. Administrator-level personnel set the permissions for each individual's account. Permissions range from station-specific access to permissions to delete documents. So, for example, an EEO Program Manager at Station X will only have access to Station X cases, not Station Y, Station Z, etc.
2. Administrator-level personnel disable any account upon receiving notice that there is personnel turnover or individuals who have access to the system no longer need (e.g., if there is an Acting EEO Program Manager who is later relieved of his or her duties). Once an account is disabled, a user cannot log in to the system. Typically, the individual, his or her supervisor, or the administration-level program offices will notify ORMDI that an individual no longer needs access.
3. Further, no individual is granted access to the system without signing a Rules of Behavior form, requiring them to uphold individuals' privacy, among other things. This form needs to be signed by the individual requesting access and by his or her supervisor.
4. CATS, accounts are automatically terminated if there is no activity for 3 months. Accounts are also removed based on ORMDI's updated listing of HR managers.
5. Errors in the dissemination of information can occur during the complaint process. To mitigate, monthly privacy messages are sent out to all ORMDI staff reviewing recent privacy events and providing suggestions to reduce the incidence of these events.

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.

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.

PII/PHI Data Element	Internal Use	External Use
Name	File Identification purposes	Not used
Personal Mailing Address	File Identification purposes	Not used
Personal Phone Number	File Identification purposes	Not used
Personal Fax Number	File Identification purposes	Not used
Personal Email Address	File Identification purposes	Not used

Race/Ethnicity	Adjudication in the EEO process	Not used
Year of birth	File Identification purposes	Not used
Memos, Letters and Emails	Adjudication in the EEO process	Not used
Affidavits	Adjudication in the EEO process	Not used
Legal Documents	Adjudication in the EEO process	Not used
Correspondence and other documents pertinent to the EEO Complaint (e.g., employment data, applications for employment, disciplinary actions, etc.)	Adjudication in the EEO process	Not used
Settlement Agreements	Adjudication in the EEO process	Not used

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

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

Upwards of 5,000 complaints per year were filed and entered into CATS until November of 2021. Open cases are still continuously updated. Data from these complaints is organized and sorted for management purposes (e.g., number of racial discrimination complaints filed at X facility, or number of complaints completed within X number of days). Also, the Senior Managers Report, a Congressionally mandated report summarizing findings of discrimination against VA's senior managers, is compiled, and submitted on a quarterly and annual basis. The system also creates the following metrics:

- System record resolution rates
- Processing time
- Savings reports
- Offer rates
- Case closure/performance metrics
- Settlement Report metrics
- Basis of Complaints
- EEO Complaint Data by type, formal/informal, location and by individuals
- Participation rates, and other EEOC data
- Emails with Notice Forms as required by law.

(No Personal data is aggregated in these reports)

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 process of EEO case adjudication creates the following information that is stored with each case and used for decision making and resolutions:

- EEO complaint form (4939)
- Memos, letters, and emails
- Affidavits
- Settlement agreements
- Legal documents (final agency decisions and actions)
- Correspondence and other documents pertinent to the EEO complaint, e.g., employment data, applications for employment, disciplinary actions, etc.

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

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

VA uses a wide variety of protections for data at rest, depending on the media. To date, only massive storage systems lack such protection; this is because the complexity of encrypting data across a data array or the conflicting requirements for speed of access versus resources consumed to encrypt it, or possibly both. VA has policies for what types of e-mail require encryption; the VA gateway will not allow unencrypted transmission of documents containing what appear to be SSNs, for example. VA laptops and, increasingly, PCs, are running the Symantec Encryption Endpoint, which includes encryption of the hard drive; only a pre-authorized VA user can log on to the device when it is removed from the VA network. RMSI systems uses encryption in place on its tape backup system, so all backup tapes created within the last two years must be read with a VA backup software server. All VA data being transmitted outside the agency on removable media (CD or DVD, for example), must be encrypted and the password must be transmitted separately to the intended storage system.

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

The system does not gather social security numbers.

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

Rules of conduct are in place and enforced for persons involved in the design, development operations or maintenance of any system of records or maintaining any records. Appropriate administration, technical and physical safeguards exist to ensure the security and confidentially of records. Access to PII is limited by the CATS application to only those data items deemed necessary to process the EEO complaints. This data is identified above, by policy and law. System documentation includes detailed system design and user guides that specify those areas of the system that contain PII, as well as how it is to be access and used by the system users. Additionally, user roles are implemented to restrict user's access to only the specific information required to perform their job function. Roles within the system are determined and requested by users, verified by a Supervisor, approved by a Manager, and added by a System Administrator.

All three administrations VHA, VBA, and NCA ensure that the practices stated in the PIA are reinforced and VA employees are required to complete all VA trainings including VA Privacy and Information Security Awareness and Rules of Behavior (VA 10176) and Privacy and HIPAA Training (VA 10203) annually. All VA employees are required to agree to all rules and regulations outlined in trainings, along with any consequences that may arise if failure to comply.

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information.

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

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

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

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

2.4a How is access to the PII determined?

Access to CATS is granted on the Least Privilege and Need to Know basis and is determined by job, discipline or business need. All ORMDI district office staff have access to data in CATS so that they can conduct their work. ORMDI's Office of Policy and Compliance staff has access to all of CATS, as do district office managers and senior leadership.

Each time an individual accesses a CATS case file it is captured in logs. Once an ORMDI staff person with access to CATS leaves ORMDI, Human Resources will notify the system administrator and access will be terminated. Furthermore, if there is no activity in a CATS account for 6 months, the account is terminated.

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

The CATS System Design Document and User Guides outline the roles and responsibilities for CATS users.

2.4c Does access require manager approval?

Requests for access to CATS can only be made by Supervisors/Managers.

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

When users log into CATS, the access is tracked and recorded in audit logs. Any changes made to the system are tracked and recorded. Basically, the CATS application has implemented auditing which tracks user access to the system and all data entered or accessed. For examples, each time a user accesses an EEO casefile, it is captured in log All changes or access to CATS case files is captured in the CATS audit logs.

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

Access to PII is limited by in CATS to only those data items deemed necessary to process the EEO case. This data is identified above, by policy and law. System documentation includes detailed system design and user guides that specify those areas of the system that contain PII, as well as how it is to be used by the system users. Additionally, user roles are implemented to restrict user's access to only the specific information required to perform their job function. Roles are determined and requested by users, approved by Supervisors, and verified by Managers with a final verification and addition a system administrator.

The CATS application has implemented auditing which tracks user access to the system and all data accessed. The information is mapped in the audit record by file identifying code. All three administrations VHA, VBA, and NCA ensure that the practices stated in the PIA are reinforced and VA employees will be required to complete all VA trainings including VA Privacy and Information Security Awareness and Rules of Behavior (VA 10176) and Privacy and HIPAA Training (VA 10203). All VA employees are required to agree to all rules and regulations outlined in trainings, along with any consequences that may arise if failure to comply.

<u>Privacy and HIPAA Training</u>
This course is available in two formats, web-based and text. Annually, all employees who have access to PHI and/or VHA computer systems during each fiscal year must complete either of these course versions to meet the mandatory training requirement. This training provides guidance on privacy practices for the use and disclosure of protected health information (PHI) and Veteran rights regarding VHA data. It contains policy implementation content as described in VHA Handbook 1605.1. There is a substitute for VA 10203: VA 10204, Print Version.

<u>VA Privacy and Information Security Awareness and Rules of Behavior</u>
VA Privacy and Information Security Awareness and Rules of Behavior (ROB) provides information security and privacy training important to everyone who uses VA information systems or VA sensitive information.

After completing this course, you will be able to identify the types of information that must be carefully handled to protect privacy; recognize the required information security practices, legal requirements, and consequences and penalties for non-compliance; and explain how to report incidents.

You must electronically acknowledge and accept the ROB to receive credit for course completion. This course fulfills the fiscal year MANDATORY annual awareness training required for all VA employees. Certificates of completion for the course apply to the Information Security and Privacy Awareness requirements and to the ROB. This course was updated October 1, 2017.

Note: You should either take the online version of this course or coordinate with your supervisor and local TMS Administrator to get credit for attending an ISO-led presentation and signing the ROB. (TMS Administrators can use item VA 832914 to record this training for learners who attend an ISO-led training. The ISO should ensure paper copies of signed ROB are retained for one year.

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*

All information listed in Section 1.1 is retained per the period determined by Record Management Schedules and OGC Hold/Freeze Lists.

3.2 How long is information retained?

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

EEO: Per General Records Schedule 2.3: EEO discrimination complaint case files are destroy per the following:

- Informal Process: Destroy 3 years after resolution of case but longer retention is authorized if required for business use: DAA-GRS-2018-0002-0012
- Formal Process: Destroy 7 years after resolution of case but longer retention is authorized if required for business use: DAA-GRS-2018-0002-0013
- Hard copy information filed in the official discrimination complaint file is retained in CATS for at least seven years after the case is closed. An exception would be when the agency's Office of General Counsel (OGC) puts a litigation hold on a case file. In this instance, the information will be retained until OGC releases its litigation hold.

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

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

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

Yes – Department of Veterans Affairs – Records Control Schedule 10-1, dated January 2021.

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

ORMDI follows Department of Veterans Affairs – Records Control Schedule 10-1, dated January 2021.
VA Handbook 5975.1, General Records Schedule (GRS) Code 20 –

- DAA-GRS-2018-0002-0012
- DAA-GRS-2018-0002-0013

https://www.archives.gov/files/records-mgmt/grs/grs02-3.pdf

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

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

It is VA policy that all Federal records contained on paper, electronic, or other medium are properly managed from record creation through final disposition, in accordance with Federal laws, the General Records Schedule and the Department of Veteran Affairs Record Control Schedule 10-1 dated January 2021. Further, Section 1 – Purpose of the VHA Records Control Schedule 10-1 states that "The Records Control Schedule (RCS) 10-1 provides Veterans Health Administration (VHA) records retention and disposition requirements for VHA Central Office,

Program Offices, and field facilities and Section 4 – Disposition of Records states that "The RCS 10-1 contains retention and disposition requirements for VHA records authorized by NARA or assigned a GRS authority. Record disposition refers to the transfer of records to an approved records storage facility, transfer of permanent records to NARA, the destruction of records, or other appropriate actions to dispose of records. Unless retrieved; records transferred to a storage facility shall be dispositioned after expiration of their retention requirements."

Within the Department of Veterans Affairs – Records Control Schedule 10-1, dated January 2021. It provides a brief description of the records and states the retention period and disposition requirements. It also provides the NARA disposition authorities or the GRS authorities, whichever is appropriate for the records, in addition to program and service sections.

Upon expiration of the data retention period, records are destroyed in accordance with VA (Handbook 6500.1 Electronic Media Sanitization Policy) and NIST (SP800-88r1 Guidelines for Media Sanitization) record retention and Media Sanitization procedures. Media in the VA environment are sanitized following VA 6500.1 Guidelines.

For each case handled by non-ORMDI personnel (i.e., Administration and Staff Office EEO managers), correspondence is received instructing them to redact non-essential PII from documents being submitted as part of the EEO case file. They have also been instructed in separate training.

ORMDI staff are trained to review all documents included in the case file for unnecessary PII and to redact it. As a second check, case managers review all files before finalizing them. Hard copy records that are held in Central Office are sent to VACO's Office of Administration's Records Manager Officer for shredding. Other district offices use VA-provided shredding services, or they contract with local shredders who provide a receipt for the shredding.

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

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

ORMDI does not use PII for research, testing or training. All documents used in training have PII redacted. When training new employees on the systems, only employees who have taken the Information Awareness and Privacy Training, and who have signed the VA National Rules of Behavior can access the system. The data contained in CATS remains the intellectual property of the system owner (VA). VA may use the data for purposes as necessary to fulfill its mission.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

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

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

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

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

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

Follow the format below:

Privacy Risk:

1. Unauthorized access to the files.
2. Information could be stored longer than necessary.

Mitigation:

1. Hard copy records are kept for no longer than is absolutely necessary, pursuant to the Federal records retention schedule. Additionally, all notes taken by counselors are destroyed after the file goes formal, and by investigators after the investigation report is completed. The risk, however, is not mitigated for electronic files because they are currently held indefinitely. Once an ORMDI staff person with access to CATS leaves ORMDI, the Division Lead or Human Resources will enter a ticket into the Help Desk System that notifies the system administrator to terminate access. Furthermore, if there is no activity in a CATS account for 6 months, the account is terminated. Access by EEO program managers (who are not ORMDI staff) who have access to EEO files in their particular geographic regions, is monitored. Their access will be terminated by lack of activity, if Form 9957 is not renewed, or by the expiration of their PIV card.
2. CATS follows VA Handbook 5975.1 and Records Control Schedule 10-1, dated January 2021. Upon expiration, all retained data will be carefully disposed, as described in Section 3.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

The following questions are intended to define the scope of information sharing/receiving/transmitting within VA.

4.1 With which internal organizations is information shared/received/transmitted? What information is shared/received/transmitted, and for what purpose? How is the information transmitted?

NOTE: Question 3.9 (second table) on Privacy Threshold Analysis should be used to answer this question.

Identify and list the names of any program offices, contractor-supported IT systems, and any other organization or IT system within VA with which information is shared.

State the purpose for the internal sharing. If you have specific authority to share the information, provide a citation to the authority.

For each interface with a system outside your program office, state what specific data elements (PII/PHI) are shared with the specific program office, contractor-supported IT system, and any other organization or IT system within VA.

Describe how the information is transmitted. For example, is the information transmitted electronically, by paper, or by some other means? Is the information shared in bulk, on a case-by-case basis, or does the sharing partner have direct access to the information?
This question is related to privacy controls AP-2, Purpose Specification, AR-3, Privacy Requirements for Contractors and Service Providers, AR-8, Accounting of Disclosures, TR-1, Privacy Notice, and UL-1, Internal Use.

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system***	***Describe the method of transmittal***
ORMDI Office of Policy and Compliance	ORMDI office responsible for compliance of EEO process	Letters, Forms (4939), emails, reports (employment data, HR, investigations, etc.), affidavits, contracts, legal documents, and decisions.	Secure HTTPS
ORMDI Office of Quality and Performance	ORMDI office responsible for oversight of the CATS system	Letters, Forms (4939), emails, reports (employment data, HR, investigations, etc.), affidavits, contracts, legal documents, and decisions.	Secure HTTPS
ORMDI FOIA and Privacy Officer	Information requests and investigation of privacy incidents	Letters, Forms (4939), emails, reports (employment data, HR, investigations, etc.), affidavits, contracts,	Secure HTTPS

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*
		legal documents, and decisions.	
ORMDI EEO Program Managers	Management purposes	Management reports only	Secure HTTPS
OCHCO	If EEO complainant accepts mediation, they become a client for alternative dispute resolution team	Name, address, email, phone number of complainants, whether or not offer of mediation is accepted or refused	Encrypted Email
ORMDI CATS	CATS auto-populates and send notices to stakeholders	Contact information, name, mailing address and zip code, phone number, email address, Race/Ethnicity, Year of birth, pertinent complaint data	Secure HTTPS
EEO Program Managers (VHA, VBA, Staff Offices)	Management purposes	Management reports only	Secure HTTPS
Office of Employment Discrimination Complaint Adjudication	Judicial review	Investigative file	Secure HTTPS
Office of the Secretary, Office of Congressional and Legislative Affairs, Office of the Undersecretary for VHA, VBA, NCA	Congressionally requested or mandated reports	Names and summaries of complaints filed against individuals in VA	Secure HTTPS
Administrations (i.e., VHA, VBA, VACO, NCA)	The field coordinates the mediations (scheduling, logistics, etc.)	Contact information, name, mailing address and zip code, phone number, email address, Race/Ethnicity, Year of birth, pertinent complaint data	Secure HTTPS

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

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

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

Follow the format below:

Privacy Risk:
1. Inadvertent disclosure.
2. Wrongful Access.
3. Information system breakdown/intrusion/penetration.
4. Requests from facility directors for information on mediation efforts not on a "need-to-know" basis.

Mitigation:
1. Awareness training and monthly privacy updates/reminders from the ORMDI privacy officer
2. Access controls - The type of access is determined and based on job, discipline, or business need. Individuals' access to casefiles is captured in logs. Password refresh is forced 90 days.
3. ORMDI operates redundant systems for failover or disaster recovery/COOP.
4. Requests of this type would come to the local EEO program manager. The request would only be shared on a "need-to-know" basis. Controls are found in the VA Rules of Behavior that all VA employees sign on an annual basis.

Section 5. External Sharing/Receiving and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to VA, which includes Federal, State, and local governments, and the private sector.

5.1 With which external organizations (outside VA) is information shared/received? What information is shared/received, and for what purpose? How is the information transmitted and what measures are taken to ensure it is secure?

Is the sharing of information outside the agency compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If not, please describe under what legal mechanism the IT system is allowed to share the information in identifiable form or personally identifiable information outside of VA.

NOTE: Question 3.10 on Privacy Threshold Analysis should be used to answer this question.

Identify and list the names of any Federal, State, or local government agency or private sector organization with which information is shared.

For each interface with a system outside VA, state what specific data elements (PII/PHI) are shared with each specific partner.

What legal mechanisms, authoritative agreements, documentation, or policies are in place detailing the extent of the sharing and the duties of each party? For example, is the sharing of data compatible with your SORN? Then list the SORN and the applicable routine use from the SORN. Is there a Memorandum of Understanding (MOU), Computer Matching Agreement (CMA), or law that mandates the sharing of this information?

Describe how the information is transmitted to entities external to VA and what security measures have been taken to protect it during transmission.

This question is related to privacy control UL-2, Information Sharing with Third Parties

Data Shared with External Organizations

List External Program Office or IT System information is shared/received with	***List the purpose of information being shared / received / transmitted with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted)with the Program or IT system***	***List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)***	***List the method of transmission and the measures in place to secure data***
Equal Employment Opportunity Commission	Judicial review	Investigative file: • name, • personal mailing address, • personal phone number, • personal fax number, • personal email address, • race/ethnicity, • year of birth, • memos, letters, and emails, • affidavits, • legal documents, • Correspondence and other documents pertinent to the EEO Employment Complaint (e.g., employment data, applications for employment, disciplinary actions, etc.), • Settlement agreements	Code of Federal Regulations Title 29, Subtitle A, Part 16 – Equal Access to Justice Act - 29 CFR §16 System of Record (SORN) 203VA08 – Department of Veterans Affairs, Office of Resolution Management, Diversity and Inclusion (ORMDI)	HTTPS

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.

If no External Sharing listed on the table above, ***(State there is no external sharing in both the risk and mitigation fields).***

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

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

Follow the format below:

Privacy Risk: The only privacy risk involved in the sharing of EEO complaint files from CATS with the EEOC occurs when files are downloaded from CATS onto a desktop computer from where they are uploaded to an EEOC IT system. The risk is if the wrong file is downloaded onto the desktop.

Mitigation: Awareness training is provided to all ORMDI employees through monthly reminders provided by the ORMDI privacy officer and in occasional training by ORMDI supervisors.

Section 6. Notice

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

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

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

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

When an aggrieved party (AP) contacts ORMDI with a possible discrimination complaint, ORMDI counselors reach out verbally to the AP to collect initial contact information and what the complaint is about. The counselor then conducts an initial interview verbally with the AP. No evidence is collected at this stage. The HIPAA Notice (Appendix 1) is sent to the AP during this stage. The HIPAA Notice clearly indicates that ORMDI will be collecting personally identifiable information and that it can only be disclosed upon the written consent of the individual. If and when the AP is ready to file a formal complaint, they are provided with VA Form 4939 (Appendix 2) to fill out which provides contact information and details the complaint(s) with which the AP wants to proceed. VA Form 4939 includes a Privacy Act Statement detailing how the information will be used and how it may be disclosed.

When the complaint goes formal, an investigation ensues, and evidence is collected. The following guidance is provided to the complainant regarding what evidence is needed: EEOC Guidelines for What it Takes to Prove Discrimination based on Sex, Race, National Origin, Color, Religion, Age, and Reprisal (Appendix 3); and EEOC Guidelines for What it Takes to Prove Discrimination based on Disability (Appendix 4).

The System of Record (SORN) 203VA08/87 FR 31058 –Diversity and Equal Employment Opportunity (EEO) Program Records – VA, Department of Veterans Affairs (VA), Office of Resolution Management, Diversity and Inclusion (ORMDI) – published 5/20/2022 - 2022-10848.pdf (govinfo.gov).

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

For notices provided see Appendices 1 through 4 to this PIA. Additional notice is provided by the System of Record (SORN) 203VA08/87 FR 31058 –Diversity and Equal Employment Opportunity (EEO) Program Records – VA, Department of Veterans Affairs (VA), Office of Resolution Management, Diversity and Inclusion (ORMDI) – 5/20/2022 - 2022-10848.pdf (govinfo.gov)

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.

When an aggrieved party (AP) contacts ORMDI with a possible discrimination complaint, ORMDI counselors reach out verbally to the AP to collect initial contact information and what the complaint is about. The counselor then conducts an initial interview verbally with the AP. No evidence is collected at this stage. The HIPAA Notice (Appendix 1) is sent to the AP during this stage. The HIPAA Notice clearly indicates that ORMDI will be collecting personally identifiable information and that it can only be disclosed upon the written consent of the individual. If and when the AP is ready to file a formal complaint, they are provided with VA Form 4939 (Appendix 2) to fill out which provides contact information and details the complaint(s) with which the AP wants to proceed. VA Form 4939 includes a Privacy Act Statement detailing how the information will be used and how it may be disclosed.

When the complaint goes formal, an investigation ensues, and evidence is collected. The following guidance is provided to the complainant regarding what evidence is needed: EEOC Guidelines for What it Takes to Prove Discrimination based on Sex, Race, National Origin, Color, Religion, Age, and Reprisal (Appendix 3); and EEOC Guidelines for What it Takes to Prove Discrimination based on Disability (Appendix 4).

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.

In the EEO complaint process, the customer is given a "Notice of Rights and Responsibilities" (Appendix 5, p. 5) to the AP in which a paragraph states: "You have the responsibility to cooperate with VA during the processing of your complaint. You must keep the VA informed of your current address; you must claim any mail sent to you, and you must cooperate with any individual assigned to the complaint. If you eventually file an appeal to the EEOC about the complaint, you must serve copies of the appeal papers on VA." APs can decline to provide information. ORMDI will process the claim, but without the necessary information, the claim will not proceed very far in the process.

6.3 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

This question is directed at whether an individual may provide consent for specific uses, or the consent is given to cover all uses (current or potential) of his or her information. If specific consent is required, how would the individual consent to each use? This question is related to privacy control IP-1, Consent.

With regards to CATS, in the Notice of Rights and Responsibilities (Appendix 5, p. 5) provided to the AP, the AP is required to "limit any formal EEO complaint you may file to those matters discussed with ORMDI, or to like or related matters (that is, matters which are directly related to those matters or which are unmistakably derived from those matters). Additionally, if you wish to amend a previously filed complaint, only matters that are like or related to the claim(s) in the pending complaint may be added. To protect your rights, discuss all claims with ORMDI before you file a formal complaint."

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

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

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

<u>Principle of Transparency:</u> Has sufficient notice been provided to the individual?

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

Privacy Risk: Risk of an ORMDI employee using complainant information for purposes other than for processing the complaint.

Mitigation: ORMDI employees sign the VA National Rules of Behavior.

Section 7. Access, Redress, and Correction

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

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

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

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

Individuals can request information from EEO case files through the Freedom of Information Act. ORMDI's FOIA Officer can be reached at: ORMDIFOIA@va.gov. Requests can also be made through the Privacy Act; however, the entire case file is exempt from the access provisions of the Privacy Act, per the SORN 203VA08/87 FR 31058 –Diversity and Equal Employment Opportunity (EEO) Program Records – VA, Department of Veterans Affairs (VA), Office of Resolution Management, Diversity and Inclusion (ORMDI) – published 5/20/2022 - 2022-10848.pdf (govinfo.gov).

Records are maintained at VA field facilities and the Office of Resolution Management, Diversity and Inclusion (ORMDI), Department of Veterans Affairs, 810 Vermont Avenue NW, Washington, DC 20420. For addresses of VA field facilities, see *www.va.gov/find-locations.*

Privacy Officer, Office of Resolution Management, Diversity and Inclusion (ORMDI), Department of Veterans Affairs, 810 Vermont Avenue NW, Washington, DC 20420, email: ormdiprivacy@va.gov.

An individual who seeks access to or wishes to contest records maintained under his or her name in this system must submit a written request to the Privacy Officer of the VA facility where the underlying incident or issue occurred.

Individuals seeking information concerning the existence and content of a record pertaining to themselves must submit a written request to or apply in person before the Privacy Officer of the VA facility where the underlying incident or issue occurred. Written requests should be signed

and contain the individual's full name, mailing address, email address, telephone number, and the case number or case title.

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)?

Requests can also be made through the Privacy Act; however, the entire case file is exempt from the access provisions of the Privacy Act, per the SORN 203VA08/87 FR 31058 –Diversity and Equal Employment Opportunity (EEO) Program Records – VA, Department of Veterans Affairs (VA), Office of Resolution Management, Diversity and Inclusion (ORMDI) – published 5/20/2022 - 2022-10848.pdf (govinfo.gov)

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?

Virtually all information gathered in an EEO complaint emanates from: (a) the aggrieved party- all information provided by the aggrieved party is voluntary; (b) witness testimony; and, (c) official documentation gathered by the local facility Human Resources manager that is verified as being true and accurate.

At the end of the formal stage of the complaint process, the complainant receives a copy of the complete investigative file – a compilation of all evidence, testimony, and correspondence during the counselling and investigative stages of the process.

Individuals can request information from EEO case files through the Freedom of Information Act. ORMDI's FOIA Officer can be reached at: ORMFOIA@va.gov. Requests can also be made through the Privacy Act; however, the entire case file is exempt from the access provisions of the Privacy Act, per the SORN 203VA08/87 FR 31058 –Diversity and Equal Employment Opportunity (EEO) Program Records – VA, Department of Veterans Affairs (VA), Office of Resolution Management, Diversity and Inclusion (ORMDI) – published 5/20/2022

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.

Ongoing EEO case files are updated as information is received, either from the complainant or from requests to the local HR office (the type of information provided depends upon the allegation(s) that have been made). ORMDI maintains district offices around the country to process EEO complaints on a regional basis:
North Atlantic District One – Lyons, NJ (908) 604-5349
North Atlantic District Two – Washington, DC (202) 632-9599
Midwest District – Hines, IL (708) 202-7072

Southeast District – St. Petersburg, FL (727) 540-3971
Continental District – Houston, TX (713) 794-7756
Pacific District – Los Angeles, CA (713) 794-7756

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.

Witness testimony is taken verbally (and transcribed), or in writing. When transcribed, the testimony is given to the witness to review and verify and then sign. In the taking of testimony, witnesses are told there is no promise of confidentiality. It is up to the complainant to ensure that the information is complete and accurate, and to provide up-to-date contact information if it changes during the investigation. If the contact information is incorrect, the complainant risks missing deadlines which are communicated in writing. By missing deadlines, the complainant risks closing the case prematurely.

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

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

In the EEO process, the complainant gets a copy of the complete investigative file at the completion of the investigation. If the complainant raises issues regarding accuracy or corrections, the complainant can request a hearing which opens the process to discovery.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

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

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

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

Follow the format below:

Privacy Risk:
1. Redress for allegations against a responsible management official.
2. If contact information is wrong, and the wrong person is contacted regarding mediating a workplace dispute, this information is released to the wrong person.

Mitigation:
1. If a complainant alleges discrimination against a supervisor (responsible management official-RMO), the RMO can only provide personal testimony against the allegations. They cannot see anyone else's testimony. If there is a finding of discrimination against the RMO, then the RMO can obtain pertinent witness testimony. If there is no finding of discrimination, all witness testimony will be withheld from the RMO. Access provisions of the Privacy Act are exempted, and FOIA protects the identities of witnesses.
2. Contact information is verified by the mediator/program manager during initial contact with participants.

Section 8. Technical Access and Security

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

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

These questions are related to privacy control AR-7, Privacy-Enhanced System Design and Development.

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

End User Access: For CATS, a request for application access is submitted to the ORMDI Helpdesk by a Manager or Supervisor, which is then forwarded to ORMDI Tier 2 Help Desk to validate or confirm the level or type of access to be granted. The ORMDI Tier 2 Help Desk reaches out and confirms with the Supervisor/Manager the appropriate level of access. This type of access level is entered into the ORMDI Help Desk ticket for implementation. The ORMDI Supervisor/Manager determines access based on job, discipline, or business need. Access to casefiles is captured in logs, and users submit signed or approved VA form 9957 when needed. The user must have completed and signed the VA National Rules of Behavior.

Specific user roles are defined for users on the CATS application. Currently, user roles are defined by business leadership. The following steps are required before any user can use the system:

- Individuals must take and pass training on privacy, HIPAA, information security, and government ethics.
- Individuals must have a completed security investigation.
- Once training and the security investigation are complete, a request is submitted for access. Before access is granted; this request must be approved by the Supervisor/Manager

Developer Access

- Developers of the CATS system are VA contractors. For details on VA contractor access, see Section 8.2.
- All individuals requesting developer access are required to complete all VA trainings (VA Privacy and Information Security Awareness and Rules of Behavior Training, Privacy and HIPAA Focused Training and Information Security for IT Specialists Training) and must be authorized by a Contractor Supervisor and the ORMDI VA Project Manager.

Personnel accessing information systems must read and acknowledge their receipt and acceptance of the VA National Rules of Behavior (ROB) or VA Contractor's ROB prior to gaining access to any VA information system or sensitive information. The rules are included as part of the security awareness training which all personnel must complete via the VA's Talent Management System (TMS). The rules state the terms and conditions that apply to personnel who are provided access to, or use of, information, including VA sensitive information, or VA information systems, such as no expectation of privacy, and acceptance of monitoring of actions while accessing the system. After the user's initial acceptance of the Rules, the user must re-affirm their acceptance annually as part of the security awareness training. Acceptance obtained through electronic acknowledgment is tracked through the TMS system. All VA employees must complete annual Privacy and Security training. CATS users agree to comply with all terms and conditions of the VA National Rules of Behavior (ROB) by signing a certificate of training at the end of the training session.

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?

Users from other agencies are not provided access to CATS as this is an internal 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.

Specific user roles are defined for users on the CATS applications system. Currently, user roles are defined by business leadership.

Access for End Users has various levels of permission from Read Only to partial to full access depending upon the need to know.

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.

Contracts for RMSI contractors are renewed annually. Contracts include OIT contract language, including security clauses and requirements for Information Security Officers, Contracting Officers, and others.

All VA contractors that have access to the pre-production environments for development purposes sign Non-Disclosure Agreements (NDAs). Contractors will also have access to the live production system for maintenance and sustainment activities. The following steps are required before contractors can gain access to the system:

- Contractors must sign a Non-Disclosure Agreement.
- Contractors must take and pass training on privacy, HIPAA, information security, and government ethics.
- Contractors must have a completed background investigation.
- Contractors accessing the RMSI system must complete relevant EPAS Training
- Once training and the background investigation are complete, an EPAS request form and a CATS system access request ticket are submitted for access.
- Access Request Tickets must be approved by the Contractors immediate supervisor and ORMDI VA Program Manager.
- The OIT System Administrator will only provide RMSI environment access upon full verification of the EPAS access request.

Contract performance and oversight is provided by the assigned contract officer representative, contract specialist and contract officers during the contract's period of performance. Most performance reports are due quarterly. Inspection and acceptance are either planned or random and based on frequency and impact errors or issues received or reported.

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.

Users of RMSI are required to take the annual Privacy Awareness training and to sign the VA Rules of Behavior. Personnel who will be accessing information systems must read and acknowledge their receipt and acceptance of the VA Rules of Behavior (ROB) or VA Contractor's ROB prior to gaining access to any VA information system or sensitive information. The rules are included as part of the security awareness training which all personnel must complete via the VA's Talent Management System (TMS). After the RMSI user's initial acceptance of the Rules, the user must re-affirm their acceptance annually as part of the security awareness training. Acceptance obtained through electronic acknowledgment is tracked through the TMS system. All VA employees must complete annual Privacy and Security training. RMSI users agree to comply with all terms and conditions of the National Rules of Behavior, by signing a certificate of training at the end of the training session.

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

8.4a If Yes, provide:

1. *The Security Plan Status:* Approved
2. *The System Security Plan Status Date:* 10-Jan-2023
3. *The Authorization Status:* Authorization to Operate
4. *The Authorization Date:* 06-Mar-2023
5. *The Authorization Termination Date:* 05-Mar-2024
6. *The Risk Review Completion Date:* 24-Feb-2023
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* Moderate

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

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

Section 9 – Technology Usage

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

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

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

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

RMSI uses the VA Enterprise Cloud – Microsoft Azure Government Cloud.

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

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.

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.

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).

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 provided in this Privacy Impact Assessment is true and accurate.

ZULEMA BOLIVAR

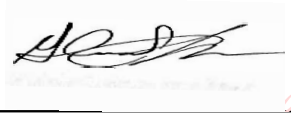
Digitally signed by ZULEMA BOLIVAR
Date: 2024.01.10 10:48:29 -05'00'

Privacy Officer, Zulema Bolivar

ANTHONY MCFARLANE

Digitally signed by ANTHONY MCFARLANE
Date: 2024.01.11 07:36:26 -07'00'

Information Systems Security Officer, Anthony McFarlane



Digitally signed by Thomas, Glenn S. (ORMDI)
Date: 2024.01.10 08:09:21 -05'00'

Information Systems Owner, Glenn Thomas

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; screen shot of a website collection privacy notice).

Appendix 1 – HIPAA Notice - Notice of Privacy Practices IB 10-163: VA Boston Health Care | Veterans Affairs

Appendix 2 – VA Form 4939 - VA Form 4939.pdf (sharepoint.com)

Appendix 3 – EEOC Guidelines

Appendix 4 – EEOC Guidelines for Disability

Appendix 5 – Notice of Rights and Responsibilities (Complainant)

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