Privacy Impact Assessment for the VA IT System called:

Resolution Management System Infrastructure

Office of Resolution Management, Diversity & Inclusion
Office of Human Resources & Administration

Date PIA submitted for review:
March 7th 2022

System Contacts:

<table>
<thead>
<tr>
<th>Role</th>
<th>Name</th>
<th>E-mail</th>
<th>Phone Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy Officer</td>
<td>Zulema Bolivar</td>
<td><a href="mailto:Zulema.Bolivar@va.gov">Zulema.Bolivar@va.gov</a></td>
<td>202-461-6932</td>
</tr>
<tr>
<td>Information System Security Officer</td>
<td>Ashton Botts</td>
<td><a href="mailto:Ashton.Botts@va.gov">Ashton.Botts@va.gov</a></td>
<td>303-398-7155</td>
</tr>
<tr>
<td>Information System Owner</td>
<td>Glenn Thomas</td>
<td><a href="mailto:Glenn.Thomas@va.gov">Glenn.Thomas@va.gov</a></td>
<td>202-461-0293</td>
</tr>
</tbody>
</table>
Abstract

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

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 purpose of the system is to replace ORMDI server systems currently housed in VA’s Cleveland, Ohio and Martinsburg, WV data centers. The system will contain two minor applications: Complaints Automated Tracking System (CATS) and the Alternate Dispute Resolution (ADR) Tracker. This is a mission-critical system necessary for the conduct of the Office of Resolution Management’s (ORMDI) day-to-day operations.

Overview

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

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

The RMSI includes infrastructure and servers that will be housed on the VA Enterprise Cloud Services “Microsoft Azure-hosted platform.” The purpose of the system is to replace ORMDI servers currently housed in Virtual Computer Equipment (VCE) known as “VCE VBlock” platform. The system will
contain two minor applications: Complaints Automated Tracking System (CATS) and the Alternate Dispute Resolution (ADR) Tracker. This system, and the applications that it supports, are necessary to the conduct of the Office of Resolution Management’s (ORMDI) day-to-day operations. 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 320 people across the country, processes more than 5,000 EEO complaints for the Department of Veterans Affairs (VA) each year. CATS is the main repository of essential documents in the equal employment opportunity (EEO) process. It assists ORMDI in its objectives to promote a healthy working environment through the prevention, resolution and processing of workplace disputes, including complaints of discrimination. It also enables ORMDI to meet the statutory deadlines for processing and adjudicating EEO complaints, and monitoring settlement agreements.

ORMDI also has the responsibility to promote and deliver alternative dispute resolution techniques for all workplace disputes in VA, including alleged equal employment opportunity (EEO) discrimination. The collection of information in ADRTracker supports the resolution of these workplace disputes. Several thousand EEO and other workplace complaints are entered into this ADRTracker application each year. The Resolution Management System Infrastructure is not shared with any other organization. It is restricted to ORMDI use. The applications housed on this system are shared with other VA organizations. All of 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. ADRTracker access is limited to ADR staff within ORMDI, and to EEO/ADR program managers in VHA, VBA, NCA and VACO staff offices. These two systems capture equal employment opportunity (EEO) and ADR – related documents (contact information, forms, letters, memos, emails, affidavits, agreements, meetings, and other correspondence) electronically and manages them. Consequently, personally identifiable information will reside on this system.

Access to ADRTracker is restricted based on the jurisdiction or facility(ies) being served by the user. For example, an EEO program manager in a VA hospital in Des Moines, IA would only have access to complaints filed in that hospital.

Regarding user account management, accounts can be automatically suspended after 3 months of no activity. Systems analysts can also view users that have logged in; they can generate a list of users with their last login date, as well as generate a report of login activities for an individual. If PII maintained in CATS or ADRTracker is inadvertently disclosed, the impact of harm incurred would be considered low. Its greatest affect would be on the reputation of ORMDI and the EEO/ADR process.

There will be no changes to ORMDI business processes because of this system. The system resides in the cloud, and FEDRAMP approval has been obtained. A contract with the cloud service provider establishes ownership rights over data and PII.

Records compiled in CATS comprise the EEOC/GOVT-1 System of Records, and records compiled in ADRTracker comprise the “Alternative Dispute Resolution Tracking System-VA” (116VA09). ORMDI is seeking VA Authority to Operate prior to the transition to the Enterprise Mission Assurance Support Service.
Section 1. Characterization of the Information

The following questions are intended to define the scope of the information requested and collected as well as the reasons for its collection as part of the program, IT system, or technology being developed.

1.1 What information is collected, used, disseminated, created, or maintained in the system?

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

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

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

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

- [ ] Name
- [ ] Social Security Number
- [ ] Date of Birth
- [ ] Mother’s Maiden Name
- [ ] Personal Mailing Address
- [ ] Personal Phone Number(s)
- [ ] Personal Fax Number
- [ ] Personal Email Address
- [ ] Emergency Contact Information (Name, Phone Number, etc. of a different individual)
- [ ] Financial Account Information
- [ ] Health Insurance Beneficiary Numbers
- [ ] Certificate/License numbers
- [ ] Vehicle License Plate Number
- [ ] Internet Protocol (IP) Address Numbers
- [ ] Current Medications
- [ ] Previous Medical Records
- [ ] Race/Ethnicity
- [ ] Tax Identification Number
- [ ] Medical Record Number
- [ ] Gender
- [ ] Integration Control Number (ICN)
- [ ] Military History/Service Connection
- [ ] Next of Kin
- [ ] Other Unique Identifying Information (list below)
Additional Information that are not listed above

- Year of Birth
- Employment data

**PII Mapping of Components**

The RMSI consists of 5 key components. 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:

**PII Mapped to Components**

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

<table>
<thead>
<tr>
<th>Database Name of the information system collecting/storing PII</th>
<th>Does this system collect PII? (Yes/No)</th>
<th>Does this system store PII? (Yes/No)</th>
<th>Type of PII (SSN, DOB, etc.)</th>
<th>Reason for Collection/Storage of PII</th>
<th>Safeguards</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Scanner</td>
<td>Y</td>
<td>Y</td>
<td>See bullets in 1.1 above</td>
<td>EEO purposes</td>
<td>SSL for the HTTP/URL VA Active Directory/PIV access VA Network Security VA Firewall SEE on Desktops physical security</td>
</tr>
<tr>
<td>File Server</td>
<td>Y</td>
<td>Y</td>
<td>See bullets in 1.1 above</td>
<td>EEO purposes</td>
<td>McAfee Data Exchange Layer – version 5.0.1.249 McAfee Agent – version 5.6.1.308 McAfee Endpoint Security – version 10</td>
</tr>
<tr>
<td>Web Server</td>
<td>Y</td>
<td>Y</td>
<td>See bullets in 1.1 above</td>
<td>EEO purposes</td>
<td>Secure Socket Layer (SSL)</td>
</tr>
</tbody>
</table>
1.2 What are the sources of the information in the system?

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

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

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

This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

Information is gathered and stored in the two applications, CATS and ADRTracker. The sources of information maintained in CATS emanates from:
- 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, reasonable accommodation records, applications for employment, disciplinary actions, etc.

Information in ADRTracker is collected from CATS. The majority of customers for ADR are complainants from the EEO process who have already provided their information to CATS. Information is also gathered directly from those customers who have not pursued the EEO process.
1.3 How is the information collected?

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

If the information is collected on a form and is subject to the Paperwork Reduction Act, give the form’s OMB control number and the agency form number.

This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

CATS information is collected:
- directly from the complainant and witnesses.
- from VA Form 4939 (OMB Control Number: 2900-0716).
- personnel-related information from HR

EEO case-specific information from CATS is auto-populated in ADRTracker. This accounts for roughly 50% of the information in ADRTracker. The remainder is collected directly from the individuals using ORMDI’s resolution services.

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

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

If the system checks for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract.

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

This question is related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.

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. The same is true for ADRTracker.

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

CATS
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
43 FR 19607 (May 9, 1978)
Exec. Order No. 12106 – Transfer of certain equal employment enforcement functions
44 FR 1053 (Jan. 3, 1979)

ADRTracker:
Title 5, United States Code, sections 571–584.
1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

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

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

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

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

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

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

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

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 who set the permissions for each individual’s account. Permissions range from station-specific access to permissions to delete documents. So, for example, an EEO-ADR Program Manager at Station X will only have access to Station X cases, not Station Y, Station Z, etc.
2. Administrator-level personnel can 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-ADR 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. For ADRTracker and 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 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.

Information collected in CATS includes:
- Name, address, phone number, email address, race/ethnicity
- EEO complaint form (4939)
- Memos, letters, and emails
- Affidavits
- Legal documents (final agency decisions and actions)
- Correspondence and other documents pertinent to the EEO complaint, e.g., employment data, reasonable accommodation records, applications for employment, disciplinary actions, etc.
- Settlement agreements
This information is included in the investigative file and is used for adjudication purposes in the EEO process if the complainant so chooses.

Information collected in ADRTracker includes:
- Names and contact information (address, phone number, email address) of complainants - for scheduling meetings
- The person allegedly responsible - for scheduling meetings
- The mediator - for scheduling meetings and follow-up
- Dates of meetings - for scheduling purposes
- Details of the allegations - for mediation and settlement purposes
- Copies of key documents in the complaint process, including settlement agreements - for compliance and documentation purposes.

Information in ADRTracker is used to track and monitor agency dispute resolution activities at the local level. Also, it is used to evaluate ADR utilization VA-wide, identify agency ADR best practices, and determine whether certain forms of ADR may be more appropriate in various types of cases.

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

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

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

This question is related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information

Upwards of 5,000 complaints per year are filed and entered into CATS. Data from these complaints are 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 ADRTracker system records resolution rates, processing time, savings reports, offer rates, participation rates, and other ADR data. No personal data is aggregated in these reports.
2.3 How is the information in the system secured?

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

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?

No

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

Rules of conduct 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 to ensure the security and confidentially of records.

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

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.

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information. How is access to the PII determined? Are criteria, procedures, controls, and responsibilities regarding access documented? Does access require manager approval? Is access to the PII being monitored, tracked, or recorded? Who is responsible for assuring safeguards for the PII?
Describe any types of controls that may be in place to ensure that information is handled in accordance with the uses described above. Example: Describe if training for users of the project covers how to appropriately use information. Describe the disciplinary programs or system controls (i.e. denial of access) that are in place if an individual is inappropriately using the information.

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

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

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

Access to CATS 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 EEO case files 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.

The System of Records Notice for ADRTracker is very clear about the uses of the information that is gathered in the ADRTracker. It lists 13 different uses of the records. The principal use is in support of the alternative dispute resolution program that seeks to resolve workplace disputes as soon as is possible.

Access is restricted to those individuals whose duties require access – EEO managers and ADR specialists. All users are required to read and sign the ADRTracker Rules of Behavior which govern the use of the system and information that is gathered (see Appendix 1).

**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
CATS

- Name
- Mailing address and zip code
- Phone number
- Email address
- Race/Ethnicity
- Year of Birth
- EEO complaint form (4939)
- Employment Data
- 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, reasonable accommodation records, applications for employment, disciplinary actions, etc.

ADRTracker:

- Names and contact information (address, phone number, email address) of complainants, the person allegedly responsible,
- the mediator,
- dates of meetings,
- details of the allegations, and
- copies of key documents in the complaint process, including settlement agreements.

Medical records are not stored on ADRTracker.

3.2 How long is information retained?

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

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

Hard copy information filed in the official discrimination complaint file is retained in CATS for at least four years after the case is closed (General Records Schedule 2.3: Employee Relations Records, Items 030-035). 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.

General ADR files, including correspondence, meeting notes, reports, evaluations, etc., must be destroyed when 3 years old. Longer retention is authorized when records are needed for agency business General Records Schedule 2.3: Employee Relations Records, Items 010-012).

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

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

ORMDI follows retention schedule GRS-1 approved by NARA and VA Central Office Records Control Schedule (RCS) 006-1, dated December 2018.

3.4 What are the procedures for the elimination of SPI?

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

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. Have policies and procedures been developed to minimize the use of PII for testing, training, and research?

This question is related to privacy control DM-3, Minimization of PII Used in Testing, Training and Research

ADR Tracker and CATS are not used for research or testing. 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.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

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

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

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

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

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

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

Follow the format below:

**Privacy Risk:** The biggest risk is unauthorized access to the files.

**Mitigation:** Records are kept no longer than is 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.
Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

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

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

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

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

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

Describe how the information is transmitted. For example, is the information transmitted electronically, by paper, or by some other means? Is the information shared in bulk, on a case-by-case basis, or does the sharing partner have direct access to the information?

This question is related to privacy controls AP-2, Purpose Specification, AR-3, Privacy Requirements for Contractors and Service Providers, AR-8, Accounting of Disclosures, TR-1, Privacy Notice, and UL-1, Internal Use.

Data Shared with Internal Organizations

<table>
<thead>
<tr>
<th>List the Program Office or IT System information is shared/received with</th>
<th>List the purpose of the information being shared/received with the specified program office or IT system</th>
<th>List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system</th>
<th>Describe the method of transmittal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Office of Policy and Compliance</td>
<td>ORMDI office responsible for compliance of EEO process</td>
<td>Letters, Forms (4939), emails, reports (medical, HR, investigations, etc.), affidavits, contracts, legal documents and decisions</td>
<td>Full access to IT system</td>
</tr>
<tr>
<td><strong>List the Program Office or IT System information is shared/received with</strong></td>
<td><strong>List the purpose of the information being shared/received with the specified program office or IT system</strong></td>
<td><strong>List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system</strong></td>
<td><strong>Describe the method of transmittal</strong></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>Office of Quality and Performance</td>
<td>ORMDI office responsible for oversight of the CATS system</td>
<td>Letters, Forms (4939), emails, reports (medical, HR, investigations, etc.), affidavits, contracts, legal documents and decisions.</td>
<td>Full access to IT system.</td>
</tr>
<tr>
<td>FOIA and Privacy Officer</td>
<td>Information requests and investigation of privacy incidents</td>
<td>Letters, Forms (4939), emails, reports (medical, HR, investigations, etc.), affidavits, contracts, legal documents and decisions.</td>
<td>Full access to IT system</td>
</tr>
<tr>
<td>EEO Program Managers (VHA, VBA, Staff Offices)</td>
<td>Management purposes</td>
<td>Management reports only</td>
<td>Access to data pertinent to their location</td>
</tr>
<tr>
<td>Office of Employment Discrimination Complaint Adjudication</td>
<td>Judicial review</td>
<td>Investigative file</td>
<td>Hard copy-mail</td>
</tr>
<tr>
<td>Alternative Dispute Resolution Tracker (ADRTracker)</td>
<td>If EEO complainant accepts mediation, they become a client for alternative dispute resolution team</td>
<td>Name, address, email, phone number of complainants; whether or not offer of mediation is accepted or refused</td>
<td>Auto-populated into the ADRTracker system</td>
</tr>
<tr>
<td>Office of the Secretary, Office of Congressional and Legislative Affairs, Office of the Undersecretary for VHA, VBA, NCA</td>
<td>Congressionally requested or mandated reports</td>
<td>In general, names and summaries of complaints filed against individuals in VA</td>
<td>Electronic and hard copy</td>
</tr>
<tr>
<td>CATS</td>
<td>CATS and ADRTracker auto-populate and send notices to stakeholders</td>
<td>Contact information, see checked boxes above, pertinent complaint data</td>
<td>Auto-population</td>
</tr>
<tr>
<td>List the Program Office or IT System information is shared/received with</td>
<td>List the purpose of the information being shared/received with the specified program office or IT system</td>
<td>List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system</td>
<td>Describe the method of transmittal</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>Administrations (i.e., VHA, VBA, VACO, NCA)</td>
<td>The field coordinates the mediations (scheduling, logistics, etc.)</td>
<td>Contact information, see checked boxes above, complaint data</td>
<td>Access limited to individuals at each station (i.e., each station can only view its particular case)</td>
</tr>
<tr>
<td>ORMDI EEO Program Managers</td>
<td>Management purposes</td>
<td>Management reports only</td>
<td>Access to data pertinent to their location</td>
</tr>
<tr>
<td>Office of the Secretary, Office of</td>
<td>Congressionally requested or mandated reports</td>
<td>In general, names and summaries of complaints filed against</td>
<td>Electronic and hard copy</td>
</tr>
</tbody>
</table>

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

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

Follow the format below:

**Privacy Risk:**
1. Inadvertent disclosure.
2. Wrongful Access; and,
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/ADR program manager. The request would only be shared on a “need-to-know” basis. Controls are found in the ADR Rules of Behavior signed by the EEO/ADR program managers, and 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

<table>
<thead>
<tr>
<th>List External Program Office or IT System information is shared/received with</th>
<th>List the purpose of information being shared / received / transmitted with the specified program office or IT system</th>
<th>List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program or IT system</th>
<th>List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)</th>
<th>List the method of transmission and the measures in place to secure data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Equal Employment Opportunity Commission</td>
<td>Judicial review</td>
<td>Investigative file</td>
<td>29 CFR §16</td>
<td>Data is downloaded to a desktop computer and then uploaded to an EEOC IT system (FEDSEP)</td>
</tr>
</tbody>
</table>

No information from ADRTracker is transmitted from the system to parties external to VA. Even contract mediators are not granted access to ADRTracker.

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

The requirements specified in the OMB memoranda are handled by VA’s Office of Information Technology (OIT). They are not controlled by ORMDI. ORMDI has a team of contractors who have access to CATS and ADRTracker. They operate under an OIT contract, the security provisions of which contain standard VA security requirements.

**5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure**

*Discuss the privacy risks associated with the sharing of information outside the Department and what steps, if any, are currently being taken to mitigate those identified risks.*
Discuss whether access controls have been implemented and whether audit logs are regularly reviewed to ensure appropriate sharing outside of the Department. For example, is there a Memorandum Of Understanding (MOU), contract, or agreement in place with outside agencies or foreign governments. Discuss how the sharing of information outside of the Department is compatible with the stated purpose and use of the original collection.

This question is related to privacy control AR-2, Privacy Impact and Risk Assessment, AR-3, Privacy Requirements for Contractors and Service Providers, and AR-4, Privacy Monitoring and Auditing

Follow the format below:

**Privacy Risk:** 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. For ADRTracker, no sharing of information occurs with organizations external to VA. No privacy risk identified.

**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 notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register.) If notice was not provided, why not?

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

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

Describe how the notice provided for the collection of information is adequate to inform those affected by the system that their information has been collected and is being used appropriately. Provide information on any notice provided on forms or on Web sites associated with the collection. This question is related to privacy control TR-1, Privacy Notice, and TR-2, System of Records Notices and Privacy Act Statements, and TR-3, Dissemination of Privacy Program Information.
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 2) 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 3) 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 4); and EEOC Guidelines for What it Takes to Prove Discrimination based on Disability (Appendix 5).

The only extraction of information from ADRTTracker that would arise would be for contact information for the Agency to communicate with the participant.

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 6, 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 regard to CATS, in the Notice of Rights and Responsibilities (Appendix 6, 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.”

For ADRTracker specifically, no consent is requested. Beyond the specific mediation being considered, only aggregate, statistical information is gathered and used. Consent from ADR participants is not requested, nor is it required, for this purpose.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

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

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

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

Principle of Use Limitation: Is the information used only for the purpose for which notice was provided either directly to the individual or through a public notice? What procedures are in place to ensure that information is used only for the purpose articulated in the notice?

This question is related to privacy control TR-1, Privacy Notice, AR-2, Privacy Impact and Risk Assessment, and UL-1, Internal Use

Follow the format below:

Privacy Risk:
1. Risk of an ORMDI employee using complainant information for purposes other than for processing the complaint.
2. No notice is provided to ADR participants for the use of ADR information. No privacy risks identified.

Mitigation:
1. ORMDI employees sign the VA National Rules of Behavior.
2. No mitigation measures needed.
Section 7. Access, Redress, and Correction

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

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

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

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

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

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 “EEOC/GOVT-1.”

For ADRTracker only contact information and the settlement agreement after it has been signed are stored. There are no set procedures, other than through the FOIA and Privacy Act, that allow individuals to gain access to their information. There is little reason for a request since they have the original settlement agreement.

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

There are no set procedures for correcting erroneous information in the ADR process. If, during a mediation, the party to a mediation sees that some information is incorrect – they will notify the mediator or program manager to correct the information. Also, participants review settlement agreements before and after they sign them. Settlement agreements are only uploaded into the database after they’ve been reviewed and executed by all the parties to the agreement.

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 course of an 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.
When the mediator or program manager is notified of the need to correct information, they enter ADRTracker to make the corrections. Alternatively, the individual can also contact ORMDI via e-mail to update or correct the information at “WorkplaceADR@va.gov.”

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

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

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

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.

If a party identifies that information in ADRTracker is incorrect, the individual can contact ORMDI to update or correct their information by e-mailing “Workplace ADR@va.gov.”

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

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

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

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

Follow the format below:

**Privacy Risk:**
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 in CATS before it is transferred to ADRTracker. 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?**

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

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

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

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

For CATS, a request for application access is submitted to the ORMDI Helpdesk, which is then forwarded to ORMDI Data Management Specialist to validate or confirm the level or type of access to be granted. The type of access level is returned to the ORMDI Helpdesk to implement. The Management Specialists determine and base access 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.

For ADRTracker, an individual requests access as a user of the system through the ORMDI Helpdesk. ORMDI requires a user to complete a Rules of Behavior (ROB) sheet signed by the user and his or her direct supervisor. The user returns the completed ROB to ORMDI and ORMDI grants the user access to the part of the system applicable to the user (typically the station he or she is responsible for) Most users only have access to the cases for their stations. Administrator users have global access.

Mediators and other ORMDI personnel who work at multiple stations will have access only to those stations where they conduct mediations.

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

No contract mediators have access to ADRTracker. VA IT contractors do have access, to make system changes or to address user issue requests, and for application maintenance.

All VA IT contractors have a type of VA Active Directory (AD) domain service account, with specific group access to various VA systems; some contractors have higher access privileges than others, meaning they have access to other systems that are managed for policy or for compliance. This type of access is for servicing the system, not for viewing data or reading user data files or files in databases, even though the capability exists.

Contract performance and oversight is provided by the assigned contract officer representatives, contract specialist and contract officers during the contract’s period of performance. Most performance reports are due quarterly. Inspection and acceptance is 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 CATS are required to take the annual Privacy and Information Security Awareness Training and to sign the VA National Rules of Behavior. Users of ADRTracker are required to read and sign a specific Rules of Behavior (ROB) Form for ADRTracker (See Attachment 1). As VA employees, they are also required to take the annual Privacy and Information Security Awareness training and to sign the VA National Rules of Behavior.

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

If Yes, provide:

1. The Security Plan Status, Approved
2. The Security Plan Status Date, 11/29/2021
3. The Authorization Status, Authorization to Operate (ATO)
4. The Authorization Date, 3/10/2022
5. The Authorization Termination Date, 3/23/2023
6. The Risk Review Completion Date, 2/23/2022
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.

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).

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.

VAEC Azure is in use.

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

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

VAEC Azure is in use.

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.

VAEC Azure is in use.
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.

VAEC Azure is in use.

9.5 If the system is utilizing Robotics Process Automation (RPA), please describe the role of the bots.

Robotic Process Automation is the use of software scripts to perform tasks as an automated process that executes in parallel with or in place of human input. For example, will the automation move or touch PII/PHI information. RPA may also be referred to as “Bots” or Artificial Intelligence (AI).

The system does not utilize Robotics Process Automation (RPA)
## Section 10. References

Summary of Privacy Controls by Family

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

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

ZULEMA BOLIVAR

Digitally signed by ZULEMA BOLIVAR
Date: 2022.04.05 09:03:18 -04'00'

Privacy Officer, Zulema Bolivar

Ashton Q Botts 671895

Digitally signed by Ashton Q Botts 671895
Date: 2022.04.05 07:23:27 -06'00'

Information System Security Officer, Ashton Botts

Digitally signed by Thomas, Glenn S. (ORMDI)
Date: 2022.04.04 22:31:58 -04'00'

Information System Owner, Glenn Thomas
APPENDIX A-6.1

Appendix 1: ADR Tracker Rules of Behavior

ADR Tracker Rules of Behavior

Appendix 2: HIPAA Notice

Appendix 3: VA4939

VA4939

Appendix 4: EEOC Guidelines
Microsoft Word - 200P-0358-2012103360EEOC_Guidelines (sharepoint.com) - EEOC Guidelines

Appendix 5: EEOC Guidelines for Disability
Microsoft Word - 200P-0358-2012103360EEOC_Guidelines (sharepoint.com) - EEOC Guidelines

Appendix 6: Notice of Rights and Responsibilities (Complainant)

Notice of Rights and Responsibilities (Complainant)