Privacy Impact Assessment for the VA IT System called:

Equal Employment Opportunity EcoSystem (EEOE), designated as “E²”.

Office of Resolution Management, Diversity & Inclusion (ORMDI)

Date PIA submitted for review:

July 27, 2021

System Contacts:

<table>
<thead>
<tr>
<th>System Contacts</th>
<th>Name</th>
<th>E-mail</th>
<th>Phone Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy Officer</td>
<td>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 (ISSO)</td>
<td>LaToya Butler-Cleveland</td>
<td><a href="mailto:LaToya.Butler-Cleveland@va.gov">LaToya.Butler-Cleveland@va.gov</a></td>
<td>202-461-6893</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 Office of Resolution Management, Diversity and Inclusion (ORMDI), Department of Veterans Affairs (VA) proposes to utilize an electronic records management system, titled “Equal Employment Opportunity EcoSystem (EEOE)” (designated as “E²”), to manage and execute the VA’s Equal Employment Opportunity (EEO) Program, Harassment Prevention Program (HPP), External Civil Rights Discrimination Complaints Program (ECP), and Reasonable Accommodation and Personal Services (RA/PAS) processes. E² is a comprehensive and secure repository for electronic records management to include identification, retrieval, maintenance, routine destruction, report generation, and compliance management. E² supports secure agency-wide collaboration and communication by connecting separate ORMDI Program Offices and facilities located in various geographic areas through the use of a secure and common platform.

ORMDI is responsible for administering the VA’s Equal Employee Opportunity (EEO) complaint process (38 CFR Parts 2 and 15 and Public Law 105-114), Harassment Prevention Program (HPP), External Civil Rights Discrimination Program (ECP), and Reasonable Accommodation/Personal Assistant Services (RA/PAS) Program. ORMDI is establishing E² to collect and maintain data to manage and execute these programs. E² is a comprehensive and secure repository for electronic records management to include identification, retrieval, maintenance, routine destruction, report generation, and compliance management. E² supports secure agency-wide collaboration and communication by connecting separate ORMDI Program Offices and facilities located in various geographic areas through the use of a secure and common platform.

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 Office of Resolution Management, Diversity & Inclusion (ORMDI) promotes a healthy working environment across the Department of Veterans Affairs (VA) (through the prevention, resolution, and processing of workplace disputes, including complaints of discrimination. 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. The DAS/RMDI administers VA's discrimination complaint process in a manner that ensures prompt, equitable, and efficient processing of discrimination complaints. In pursuit of these objectives, Equal Employment Opportunity Ecosystem (EEOE) was created to combine Complaints Automated Tracking System (CATS). EEOE provides the ability for the VA's Office of Resolution Management, Diversity & Inclusion ORMDI to track and process informal and formal EEO Complaints and HPP (Harassment Prevention Program) cases. Complaints submit requests and complaints through the application, which are then managed in the Dynamics 365 Online via entry screens, workflow processes, email notifications, document (letter) templates, a shared document repository, and common reporting architecture.

EEOE is the main repository of essential documents in the EEO complaint process.

Legal authority to operate EEOE is found in:

• Title 1 of the Americans with Disabilities Act of 1990 and the ADA Amendments Act of 2008 (ADAAA)
• Title 29 United States Code (U.S.C.), Sections 791, 792, and 793
• Code of Federal Regulations (CFR), Sections 1611, 1614, and 1630
• Title 38, United States Code (U.S.C.), Part I, Chapter 3, Department of Veterans Affairs, Chapter 5, Authority and Duties of the Secretary, and Chapter 7, Employees
• Title 38, Code of Federal Regulations, Chapter 1, Parts 15 and 18
• Public Law 105-114, Veterans’ Benefits Act of 1997, Title 1 – Equal Employment Opportunity in the Department of Veterans Affairs
• 42 U.S.C. § 2000d, Title VI, Civil Rights Act of 1964
• 29 C.F.R. § 1614, Federal Sector Equal Employment Opportunity
• 29 C.F.R. § 1630, Regulations to Implement the Equal Employment Provisions of the Americans with Disabilities Act
• 29 U.S.C., § 633, Age Discrimination in Employment
• 29 U.S.C. § 791; Sections 501, 504, and 505 of the Rehabilitation Act of 1973 (Public Law 93-112)
• 38 C.F.R., Part 2 and 15, Delegation of Authority – Equal Employment Opportunity (EEO) Responsibilities
• 38 C. F.R., Part 15 – Enforcement of Nondiscrimination on the Basis of Handicap in Programs or Activities Conducted by the Department of Veterans Affairs
• 38 C.F.R., Part 18 – Nondiscrimination in Federally-Assisted Programs of the Department a of Veterans Affairs – Effectuation of Title VI of the Civil Rights Act of 1964
• 45 C.F.R. Subpart D – Discrimination on the Basis of Sex in Education Programs or Activities Prohibited, § 86.31, Education programs or activities
• 42 U.S.C. § 6101-6107, Age Discrimination Act of 1975
• Executive Order 13548 -- Increasing Federal Employment of Individuals with Disabilities
• Executive Order 13164, Requiring Agencies to Establish Procedures to Facilitate the Provision of Reasonable Accommodation
• EEOC Notice 915.002 dated June 18, 1999, Enforcement Guidance on Vicarious Employer Liability for Unlawful Harassment by Supervisors
• EEOC Guidance on the ADAA
• EEOC Regulations to Implement the Equal Employment Provisions of the Americans with Disabilities Act, as Amended (29 CFR 1630 Appendix)
• EEOC Policy Guidance on Executive Order 13164, Requiring Agencies to Establish Procedures to Facilitate the Provision of Reasonable Accommodation
• EEOC Enforcement Guidance: Reasonable Accommodation and Undue Hardship under the Americans with Disabilities Act
• VA Handbook 5975.1, Processing Requests for Reasonable Accommodation from Employees and Applicants with Disabilities
• VA Directive 5979, Harassment Prevention Policy
• VA Handbook 5979, Harassment Prevention Procedures
• VA Directive 5977 EEO Complaints Process
• VA Handbook 5977, EEO Complaints Process

EEOE is a nationwide web-based content management system that enables ORMDI’s EEO staff to capture EEO-related documents electronically and manage them. 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. EEOE creates and manages electronic folders that contain the essential EEO documents, emails, and metadata. It controls access to folders and records, and maintains an auditable track of actions taken. It also provides access to an easy-to-use electronic document library. With more than 5,000 complaints entered each year, there are approximately 36,000 records currently maintained in the system.

All of ORMDI’s EEO operational staff around the country have access to EEOE, as do the EEO program managers in Administration facilities across the country and Staff Offices VA’s Office of Employment Discrimination Complaint Adjudication in Washington, DC also has access. Access to the system 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. Only ORMDI staff trained on the system can add documents. For disaster recovery purposes, the application resides in Cleveland, OH and in Martinsburg, WV. VA EEO is replicated to the secondary location in Martinsburg.

The system name is the Reasonable Accommodation Management System (RAMS), owned by Department of Veteran Affairs, Office of Resolution Management (ORM). The purpose of the program is to allow the VA to collect and maintain temporary records on employees with disabilities and applicants for employment, who are receiving reasonable accommodations as required by the Rehabilitation Act of 1973 and the Americans with Disabilities Act (ADA) Amendments Act of 2008 (ADAAA). Annually, the system will be expected to store approximately 5,000 names and Protected Health Information (PHI)
and on Department of Veteran Affairs employees enterprise wide. The RAMS system will be used enterprise wide across all three administrations. The system will be based on a Customer Relationship Management (CRM), cloud-based platform ensuring the consistent handling of PHI and PII across the site. There is not an anticipated change of business processes based on the completion of this PIA. There are no anticipated technology changes based on the completion of this PIA. This system is being created as a new program, and an initial SORN is out for final signature approvals. The VA is the owner of all data in the RAMS application, including PII, as established under the Microsoft – Dynamics CRMOL Cloud Services contract. The Dell/Microsoft Enterprise Agreement contract information is as follows: Contract Number: GS-35F-0884P; Task Order Number: VA118-17-F-1888. The period of performance is from April 1, 2017 through March 31, 2022, under the assumption that all four option year periods will be exercised. The contract is currently under the base year period set to conclude March 31, 2018.

The RAMS application is hosted on the Microsoft – Dynamics CRM (Dynamics 365) Online(CRMOL) for Government Cloud. It is a Software-as-a-Service (SaaS) offering as defined in NIST SP800-145. Both the primary and backup data centers are owned by Microsoft, who is the VA contracted Cloud Service Provider (CSP) at those sites with direct connections to the VA TIC (Trusted Internet Connection) from each respective location. The magnitude of potential harm to the employee if privacy-related data is disclosed is low to moderate due to the potential for identity theft or the unauthorized release of PHI. An unauthorized privacy-related data disclosure could negatively affect the reputation of both VA, as well as cause a reduction of public trust.

Legal Authorities to Operate:

- Rehabilitation Act of 1973
- Executive Order 13164 Establishing Procedures to Facilitate the Provision of Reasonable Accommodation
- 29 CFR 1614.203 – Rehabilitation Act
- VA Handbook 5975.1 Processing Requests for Reasonable Accommodation from Employees and Applicants with Disabilities
- VA Directive 6300, Records and Information Management
- VA Handbook 6500, VA 6500 AC-8 – System Use Notification
- The Privacy Act of 1974
- The System of Record (SORN) #203VA08 – Pending Approval
  - 09VA05 – Employee Unfair Labor Practice Charges and Complaints, Negotiated Agreement Grievances and Arbitrations - VA
  - 106VA17 – Compliance Records, Response and Resolution of Reports of Persons Allegedly Involved in Compliance Violations - VA

Recent major enhancements allow ORMDI’s system analysts to review all user activity and suspend a user account if necessary. Accounts can now be automatically suspended after 6 months of no activity. Systems analysts can also now view users that have logged in; they can generate a list of users with their last login date, as well as a report of login activities for an individual.
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://vaow.va.gov/vapubs/). If the system creates information (for example, a score, analysis, or report), list the information the system is responsible for creating.

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

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

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

- Other information: Station or Office number, government phone and email numbers, Series and Grade information, processing notes, VA Forms 0857 series, health care provider limitations, health care provider recommendations, employee/representative emails associated with the case file, legal opinions and supporting documentation on Agency decisions. The employee may submit their own medical support and records which may contain their address and data of birth. The employee can redact this information before submitting the addition medical documentation.
- 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..
- Names and contact information (address, phone number, email address) of complainants
- The person allegedly responsible
- The mediator
- Dates of meetings
- Details of the allegations
- Copies of key documents in the compliant process, including settlement agreements (Medical records are not stored in EEOE)
- Business address
- Position
- Facility
- Facility address
- Facility phone number
- Date of Request
- Information concerning issue/claim
- Any record relevant to the allegations.
- Recommendation for future harassment prevention
- Budget, Human Resources HR Employee Recruitment and Credit Card application and supporting documents.
- Facility/Administrative Space Requirements

Information created by EEOE:
- System record resolution rates
- Processing time
- Savings reports
- Offer rates
- Participation rates, and other EEOE data
  (No Personal data is aggregated in these reports)

PII Mapping of Components

Equal Employment Opportunity Ecosystem consists of one key component (databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by Equal Employment Opportunity Ecosystem 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.
### Database Name of the Information System Collecting/Storing PII

<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>Power Apps Dataverse SaaS (VA ORMDI Prod)</td>
<td>yes</td>
<td>yes</td>
<td>Employee name</td>
<td>Contact Information, Case details, Fiscal Budgeting, Process the Reasonable Accommodation Request</td>
<td>Data is encrypted in transit and at rest. Access to the system is limited; access is audited</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>First Name, Last Name, Address, Email Addresses, Phone Number, DOB Business address Position Facility Facility address Facility phone number Date of Request Information concerning issue/claim Specifics of the EEO complaint (harassment, discrimination, etc.) Legal agreements Witness testimony Health information if necessary (e.g., disability related) RAMS does collect data that is HIPPA protected. Any record relevant to the allegations. Recommendation for future harassment prevention Budget, Human Resources HR Employee Recruitment and Credit Card application and supporting documents. Facility/Administrative Space Requirements</td>
<td></td>
<td></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.

- 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
- Sources of information are: Information provided directly from the Global Listing Address (GAL), Veteran Benefits Administration (VBA), Veterans Health Administration (VHA), National Cemetery Administration (NCA), employee, information obtained from medical documentation provided by the employee, information obtained from the 0857 series forms that have been provided by the employee.
- Request and Interaction data come from system users who gather the data in the process of servicing employees.
- The source of PII from a CRM perspective is the Web Services layer, the data will Reasonable Accommodation Coordinator (RAC) will enter PHI/PII into the system (e.g. correct contact phone number) and Designated Management Official (DMO) will make the determination. NRAC or their representative may also make comments during the 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.
Information is collected:

- Directly from the complainant and witnesses;
- VA Form 4939 (OMB Control Number: 2900-0716);
- Personnel-related information from HR
- Sources of information are: Information collected directly from the employee via face to face, email, phone call and or third party, information collected from medical documentation provided by the employee, information collected from the 0857 series forms that have been provided by the employee.
- VA Form 0857A – OMB 2900-0767
- VA Form 0857K – OMB 2900-0767
- During or shortly after the interactive discussion with the employee, authorized users will access RAMS and complete necessary portions of the request to record information pertaining to the request.

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.

Information 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.

This is an internal system to be used enterprise wide across the Department of Veteran Affairs three administrations. Employees make requests via government email, government phone lines, verbally to their supervisor or through a representative. There is no third-party system check as long as the person provides the needed information to process the request as required by law. The employee basic data will be pulled from the Global Address List (GAL).

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

EEOE uses the following legal authorities, arrangements and agreements to define the collection of information:

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)
Rehabilitation Act of 1973
Americans with Disabilities Act (ADA) Amendments Act of 2008 (ADAAA), Executive Order 13164 Establishing Procedures to Facilitate the Provision of Reasonable Accommodation
29 CFR 1614.203 – Rehabilitation Act
VA Handbook 5975.1 Processing Requests for Reasonable Accommodation from Employees and Applicants with Disabilities
VA Directive 6300, Records and information Management
VA Handbook 6500, VA 6500 AC-8 – System Use Notification
The Privacy Act of 1974
The System of Record (SORN) #203VA08 – Pending Approval
The System of Record (SORN) #09VA05 – Employee Unfair Labor Practice Charges and Complaints, Negotiated Agreement Grievances and Arbitrations - VA
The System of Record (SORN) #106VA17 – Compliance Records, Response and Resolution of Reports of Persons Allegedly Involved in Compliance Violations - VA
The System of Record (SORN) EEOC/GOVT- 1 – Equal Employment Opportunity in the Federal Government Complaint and Appeals Records

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
3. System operators could input the wrong information or process the request to the wrong stakeholder for action.

**Mitigation:**
1. Risk is manifested during the processing of complaints. Errors in the dissemination of information 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.
2. If there is no activity in an account for 6 months, the account is automatically terminated. Accounts are removed based on ORMDI’s updated listing of HR managers.
3. Design team has developed script and coding to use the Global address listing (GAL) to streamline processing and minimize data input errors. All employees have access to ensure their information is correct in the GAL. The employee would need to request a help desk ticket to make changes.

**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.
This is an internal system to be used enterprise wide across the Department of Veteran Affairs three administrations. Employees make requests via government email, government phone lines, verbally to their supervisor or through a representative. There is no third-party system check as long as the person provides the needed information to process the request as required by law.

The records will include information from all VA 0857 forms and additional medical documentation provided by the Health Care Provider.

Employee or applicant of employment’s name: Form Is identified by Name
Date of Request : for tracking details of reasonable accommodation request, such as: The type of accommodation; how the accommodation will assist the applicant or employee in performing the essential functions of the job; whether the request was granted as requested, or an alternate accommodation was offered, or if the request was denied, if denied the reason for denial medical information found on VA Form 0857 forms (limitation, diagnosis, prognosis, type of accommodation): Determine eligibility and needs information concerning the nature of the disability and the need for accommodation, to include appropriate medical documentation when the disability and/or need for accommodation is not obvious

Information collected includes:
o Name, address, phone number, email address, race/ethnicity
o EEO complaint form (4939)
o Memos, letters, and emails
o Affidavits
o Legal documents (final agency decisions and actions)
o Correspondence and other documents pertinent to the EEO complaint, e.g., employment data, reasonable accommodation records, applications for employment, disciplinary actions, etc.
o 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. All records collected are available for the uses listed below.
a. To disclose pertinent information to the appropriate federal, state, or local agency responsible for investigating, prosecuting, enforcing, or implementing a statute, rule, regulation, or order, where the disclosing agency becomes aware of an indication of a violation or potential violation of civil or criminal law or regulation.
b. To disclose information to another federal agency, to a court, or to a party in litigation before a court or in an administrative proceeding being conducted by a federal agency when the government is a party to the judicial or administrative proceeding.
c. To provide information to a congressional office from the record of an individual in response to an inquiry from that congressional office made at the request of that individual.
d. To disclose to an authorized appeal grievance examiner, formal complaints examiner, administrative judge, equal employment opportunity investigator, arbitrator or other duly authorized official engaged in investigation or settlement of a grievance, complaint or appeal filed by an employee.
e. To disclose, in response to a request for discovery or for appearance of a witness, information that is relevant to the subject matter involved in a pending judicial or administrative proceeding.
f. To disclose to officials of state or local bar associations or disciplinary boards or committees when they are investigating complaints against attorneys in connection with their representation of a party before the Equal Employment Opportunity Commission (EEOC).
g. To disclose to a Federal agency in the executive, legislative, or judicial branch of government, in response to its request information in connection with the hiring of an employee, the issuance of a security clearance, the conducting of a security or suitability investigation of an individual, the classifying
of jobs, or the lawful statutory, administrative, or investigative purpose of the agency to the extent that the information is relevant and necessary to the requesting agency's decision.
h. To disclose information to employees of contractors engaged by an agency to carry out the agency's responsibilities under 29 CFR part 1614.
i. To disclose information to potential witnesses as appropriate and necessary to perform the agency's functions under 29 CFR part 1614.

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 EEOE. Data from these complaints are organized and sorted for management purposes (e.g. number of racial discrimination complaints filed at X facility). 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.

Each Reasonable Accommodation case is stand alone and the PHI, PII associate with each case will not be cross referenced by any program. The RAMS system will use Microsoft Power BI (Business Intelligence) and Excel to access general information and create reports (tallies only) on timeliness, trend analysis, costs, and over all legal compliance.

2.3 How is the information in the system secured?

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

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

This question is related to security and privacy controls SC-9, Transmission Confidentiality, and SC-28, Protection of Information at Rest
Access to PII is limited by the RAMS application to only those data items deemed necessary to process the reasonable accommodation requests. 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 and PHI, as well as how it is to be used by the RAMS. 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 to be verified and added by a system administrator within each administration. User access is managed and supervised by RAMS Administrators following receipt of request from appropriate individuals. The RAMS application implements auditing which tracks user access to the system and all data accessed. The information is mapped in the CRM 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.

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.

Add answer here:

Access to EEOE is determined by job, discipline or business need. All ORMDI field office staff and all VA EEO Program Managers have access to data in EEOE specific to their regions, so that they can conduct their work. ORMDI’s Office of Policy and Compliance staff has access to all of EEOE, as do field operations managers and senior leadership. The Administration and Staff Office EEO program managers have the ability to generate reports on certain data fields in the system. All non-ORMDI employees or staff who have access to the system submit a signed or approved VA Form 9957 (Access Form)
Each time an individual accesses EEO casefiles it is captured in logs.
Access to PII is limited by the RAMS application to only those data items deemed necessary to process the reasonable accommodation requests. 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 and PHI, as well as how it is to be used by the RAMS. 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 to be verified and added by a system administrator within each administration. User access is managed and supervised by RAMS Administrators following receipt of request from appropriate individuals. The RAMS application implements auditing which tracks user access to the system and all data accessed. The information is mapped in the CRM 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.

**Privacy and HIPAA Training**

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.

**VA Privacy and Information Security Awareness and Rules of Behavior**

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 2018 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.)

Also see Section 8: Technical Access and Security.
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

- 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..

The information which is retained is below:

- Name
- DOB
- Race/Ethnicity
- Personal Mailing Address
- Personal Fax Number
- Work Address
- Email
- Phone Number
- Previous Medical Records

All information pertaining to the case is retained as long as the individual is still assigned to the Department of Veterans Affairs. Once an employee departs the Department of Veteran Affairs, the case information will be maintained for three years IAW the following:

- Privacy Act of 1974
- 29 CFR 1611 - Privacy Act Regulations
- EEOC Order 150.003 - EEOC Privacy Act of 1974 (as amended)
- VA information security and privacy policies, including VA Handbook 6500 (Information Security Program). VA Handbook 6500
- Processing requests for reasonable accommodation from employees and applicants with disabilities. VA Handbook 5975.1
  - General Records Schedule (GRS) Code 20 - Disposition Authority DAA-GRS-2015-0007-0004

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 EEOE for at least four 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. ORMDI is currently in the process of deleting electronic files according to the records retention schedule.

All information pertaining to the case is retained as long as the individual is still assigned to the Department of Veterans Affairs. Once an employee departs the Department of Veteran Affairs, the case information will be maintained for three years IAW the following:

- Privacy Act of 1974
- 29 CFR 1611 - Privacy Act Regulations
- EEOC Order 150.003 - EEOC Privacy Act of 1974 (as amended)
- VA information security and privacy policies, including VA Handbook 6500 (Information Security Program). VA Handbook 6500
- Processing requests for reasonable accommodation from employees and applicants with disabilities. VA Handbook 5975.1
  - General Records Schedule (GRS) Code 20 - Disposition Authority DAA-GRS-2015-0007-0004

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’s OI&T Records Control Schedule dated 08/03/09 which refers to NARAs general records schedules.
Retention three years after the employee leaves the agency.

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*

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 General Records Schedule (GRS) Code 20 - Disposition Authority DAA-GRS-2015-0007-0004. 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.

Temporary documents are scanned onto optical disks and retained for 10 years. 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. Media in the Microsoft CRM and government cloud are sanitized in accordance with NIST SP800-88r1 as audited by FedRAMP).

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*
ORMDI does not use PII for research, testing or training. Data that EEOE uses from CRM is not used for research, testing, or training. The data contained in Microsoft Dynamics 365 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.

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. The biggest risk is unauthorized access to the files.
2. There is a risk that 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 EEOE leaves ORMDI, Human Resources will notify the system administrator and access will be terminated. Furthermore, if there is no activity in a EEOE 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. EEOE follows VA Handbook 5975.1, General Records Schedule (GRS) Code 20 and all records are stored for 3 years. Upon expiration, all retained data will be carefully disposed, as described in 3.4.
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 3.10 (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 shared/received with the Program Office or IT system</th>
<th>Describe the method of transmittal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Veterans Benefits Administration</td>
<td>New Case Alert</td>
<td>Contact information, case details</td>
<td>SharePoint Email notification sent for each new case to log into SharePoint</td>
</tr>
<tr>
<td></td>
<td>Benefits eligibility and issue resolution</td>
<td>Personally Identifiable Information (PII), Protected Health Information (PHI), and Individually Identifiable Information (III).</td>
<td>Direct input by stakeholders into the CRM cloud based system</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 shared/received 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>Veterans Health Administration</td>
<td>New Case Alert</td>
<td>Contact information, case details</td>
<td>SharePoint Email notification sent for each new case to log into SharePoint Direct input by stakeholders into the CRM cloud based system</td>
</tr>
<tr>
<td>The Department of Veterans Affairs Central Office</td>
<td>New Case Alert</td>
<td>Contact information, case details</td>
<td>SharePoint Email notification sent for each new case to log into SharePoint Direct input by stakeholders into the CRM cloud based system</td>
</tr>
<tr>
<td>National Cemetery Administration</td>
<td>New Case Alert</td>
<td>Contact information, case details</td>
<td>SharePoint Email notification sent for each new case to log into SharePoint Direct input by stakeholders into the CRM cloud based system</td>
</tr>
<tr>
<td>Office of Information Technology</td>
<td>New Case Alert</td>
<td>Contact information, case details</td>
<td>SharePoint Email notification sent for each new case to log into SharePoint Direct input by stakeholders into the CRM cloud based system</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

**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, all non ORMDI employees or staff must submit signed or approved VA form 9957.
3. ORMDI operates redundant systems for failover or disaster recovery/COOP.

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 3.11 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
### List External Program Office or IT System information is shared/received with

<table>
<thead>
<tr>
<th>List the purpose of information being shared/received or transmitted with the specified program office or IT system</th>
<th>List the specific PII/PHI data elements that are shared/received 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>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

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

Not Applicable

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 EEOE. 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:**

1. The only privacy risk involved in the sharing of EEO complaint files from EEOE with the EEOC occurs when files are downloaded from EEOE 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.

2. PII or PHI maybe shared with unauthorized parties.
Mitigation:
1. Awareness training is provided to all ORMDI employees through monthly reminders provided by the ORMDI privacy officer and in occasional training by ORMDI supervisors.

2. The EEOE system has authentication and authorization processes which ensures that only authorized parties can see the data. Furthermore, there is currently no sharing of data externally.

The risks and mitigation strategies described in this section cover all the information (and information types) listed in section 1.1 of this document.

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 (Attachment 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 aggrieved party is ready to file a formal complaint, they are provided with VA Form 4939 (Attachment 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 (Attachment 3); and EEOC Guidelines for What it Takes to Prove Discrimination based on Disability (Attachment 4).
In regard to medical information, VA provides a Notice of Privacy Practice which details how medical information of Veterans, other beneficiaries who receive health care benefits from VHA, and non-Veteran patients who receive benefits from the VHA. Additional notice is provided by the system’s SORN #203VA08. A third form of notice is provided by this Privacy Impact Assessment, which is available online as required by the eGovernment Act of 2002, Pub.L. 107–347§208(b)(1)(B)(iii).

The Notice of Privacy Practices can be located at

Notice of Privacy Practices IB 10-163

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, we provide a “Notice of Rights and Responsibilities” (Attachment 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.

The RAMS portion of EEOE system is based by name as listed in the GAL. SSNs are not collected. If employees refuse to provide the requested medical information, their accommodation request will be administratively closed as outlined by VA Handbook 5975.1 Processing Requests for Reasonable Accommodation from Employees and Applicants with Disabilities.

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

In the Notice of Rights and Responsibilities (Attachment 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.”
RAMS- N/A. Individuals do not have rights to consent to particular uses of information.

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. Insufficient notice is provided to the Veteran.

**Mitigation:**
1. ORMDI employees sign the VA National Rules of Behavior.
2. Notice is given by the SORN #203VA08 in Section 6.1.

**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 67 FR 49338 “EEOC/GOVT-1.”

For RAMS the individual can request their Reasonable Accommodation File by contacting their RAC.

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

For RAMS, the information collected from individuals contact the RAC is used primarily tracking. If the individual discovers that incorrect information was provided during intake, they simply follow the same contact procedures as before, and state that the information they are now providing supersedes the information previously provided. The RAC would make appropriate changes to the system as requested and all entries are logged and tracked automatically be the system.
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.

For RAMS, this normally doesn’t apply, since this information is pulled directly from the GAL. Unless the individual changes their information in the GAL or provides new medical documentation for requirements/needs, their information will not change.

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

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

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

The 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 up the process to discovery.

The individual can request their information per the FOIA.
VA Handbook 5975.1 Processing Requests for Reasonable Accommodation from Employees and Applicants with Disabilities.

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. There is a risk that the information on file is incorrect and individuals are unaware of how to access, redress, or correct their information. RAMS CSRs or EED staff members may not adhere to information security requirements instituted by the VA OIT.

**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. Individuals are notified verbally as well as able to submit VA Form 10-5345a to access their information. They can also follow the steps in VA Handbook 1605.1 to amend their information. Both contractor and VA employees are required to take annual Privacy, HIPAA, and information security training. For further details, see Section 8: Technical Access and Security.

**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.

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.

Specific user roles are defined for users on the RAMS system. CSRs, Supervisors, and Facility POCs have various user roles which define which areas of the system they can see or edit. 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 a supervisor, the appropriate Information Security Officer (ISO), and OIT.

**Developer Access**

Developers of the EEOE system are VA contractors. For details on VA contractor access, see Section 8.2.

**End-User and Tester Access**

All individuals requesting End-User and Tester 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 VA Project Manager. To ensure that this requirement is met, the designated VA Project POC must submit a signed Access Request Form for an individual or a group. At minimum, the following information should be provided for each VA Project Team member requesting access to the RAMS Environments: First Name, Last Name, Primary E-mail, Main Phone, Manager, Current date of completion annual required VA Training, last four digits of their Social Security Number, VA Employee or Contractor, VA Active Directory Username, Environment, Access Permissions, and Contract End date.

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. EEOE 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.

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 VA Project Manager. To ensure that this requirement is met, the designated Veterans Centered Experience (VCE) project Point of Contact (POC) must submit a signed Access Request Form for an individual or a group. At minimum, the following information should be provided for each VA Project Team member requesting access to the RAMS environments: First Name, Last Name, Primary E-mail, Main Phone, Manager, Current on VA Training, VA Employee or Contractor, VA Active Directory Username, Environment, Access Permissions, and Contract End date.

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 EEOE-related 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 activities. The following steps are required before contractors can gain access to the system:

- Contractors must take and pass training on privacy, HIPAA, information security, and government ethics.
- Contractors must have a completed background investigation.
- Once training and the background investigation are complete, a request is submitted for access. Before access is granted, this request must be approved by the supervisor, Information Security Officer (ISO), and OIT.

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 EEOE 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 EEOE 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.

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

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

If Yes, provide:

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

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

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

EEOE was awarded a 180 ATO on May 6, 2021. The system is migrating from on premise to the Cloud Service Provider Microsoft -Azure Government (including Dynamics 365). This system is a SaaS solution on Dynamics 365. EEOE eMASS ID #945 EEOE is scheduled to go into production in September 2021.

1. The Security Plan Status – Not Yet Approved
2. The Security Plan Status Date,
3. The Authorization Status - Authorized to Operate (ATO)
4. The Authorization Date – 6 May 2021
5. The Authorization Termination Date – 2 Nov 2021
6. The Risk Review Completion Date – 3 May 2021
7. The FIPS 199 classification of the system - MODERATE. EEOE was recategorized 11/4/2020. Categorization included the updated data types for EEOE and MSD. See eMASS for more details.
Section 9 – Technology Usage

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

9.1 Does the system use cloud technology?

*If so, Does the system have a FedRAMP provisional or agency authorization? If the system does use cloud technology, but does not have FedRAMP authorization, explain how the Cloud Service Provider (CSP) solution was assessed and what FedRAMP documents and processes were used for the assessment in order to comply with VA Handbook 6517.*

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

EEOE a SaaS cloud model which is housed on the FedRAMP approved FISMA High Microsoft Azure Government (includes Dynamics 365) – Dynamics 365 SaaS environment.

9.2 Identify the cloud model being utilized.

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

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

EEOE is a Software as a Service (SaaS).

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

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

EEOE and VA have ownership rights over data including PII. Please see the Contract between Dell Financial services and VA. This is a contract which covers the Microsoft Azure Government (includes Dynamics 365) FedRAMP connection. EEOE does not have access to the contract at the project level. Veterans Affairs does have access to this contract.

9.4 Will the CSP collect any ancillary data and if so, who has ownership over the ancillary data?
Per NIST 800-144, cloud providers hold significant details about the accounts of cloud consumers that could be compromised and used in subsequent attacks. Ancillary data also involves information the cloud provider collects or produces about customer-related activity in the cloud. It includes data collected to meter and charge for consumption of resources, logs and audit trails, and other such metadata that is generated and accumulated within the cloud environment.

This question is related to privacy control DI-1, Data Quality.

All Data ancillary or otherwise is the property of EEOE and the Veterans Affair.

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

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

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

The system will be based on a Customer Relationship Management (CRM), cloud-based platform ensuring the consistent handling of PHI and PII across the site. The VA is the owner of all data, including PII, as established under the Microsoft – Dynamics CRMOL Cloud Services contract. The Dell/Microsoft Enterprise Agreement contract information is as follows: Contract Number: GS-35F-0884P; Task Order Number: VA118-17-F-1888. The period of performance is from April 1, 2017 through March 31, 2022, under the assumption that all four option year periods will be exercised. EEOE is hosted on the Microsoft – Dynamics CRM (Dynamics 365) Online (CRMOL) for Government Cloud. It is a Software-as-a-Service (SaaS) offering as defined in NIST SP800-145. Both the primary and backup data centers are owned by Microsoft, who is the VA contracted Cloud Service Provider (CSP) at those sites with direct connections to the VA TIC (Trusted Internet Connection) from each respective location. The magnitude of potential harm to the employee if privacy-related data is disclosed is low to moderate due to the potential for identity theft or the unauthorized release of PHI. An unauthorized privacy-related data disclosure could negatively affect the reputation of both VA, as well as cause a reduction of public trust.

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

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

EEOE is not using Robotic Process Automation (RPS) at this time.
### 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: 2021.10.20 15:35:26 -04'00'

Privacy Officer, Zulema Bolivar

LaToya N. Butler-Cleveland 204980
Digitally signed by LaToya N. Butler-Cleveland 204980
Date: 2021.10.20 14:15:17 -04'00'

Information System Security Officer, LaToya Butler - Cleveland

Information System 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).

Notice of Privacy Practices IB 10-163