Privacy Impact Assessment for the VA IT System called:

Discrimination Complaint Legal Automation Workload System (DCLAWS)

VA Central Office

Office of Employment Discrimination Complaint Adjudication (OEDCA)

eMASS #2390

Date PIA submitted for review:

01/30/2024

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Taylor S. Banks	Taylor.Banks@va.gov	202-461-4050
Information System Security Officer (ISSO)	Keneath Coleman	Keneath.Coleman@va.gov	202-461-5122 / C: 202-437-1860
Information System Owner	Kalpana Ramireddy	Kalpana.Ramireddy@va.gov	202- 550-6382

Abstract

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

Discrimination Complaint Legal Automation Workload System (DCLAWS) supports the activities of VA's Office of Employment Discrimination Complaint Adjudication (OEDCA), and required reporting.

Overview

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

1 General Description

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

Discrimination Complaint Legal Automation Workload System (DCLAWS) is owned by VA's Office of Employment Discrimination Complaint Adjudication (OEDCA).

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

Discrimination Complaint Legal Automation Workload System (DCLAWS) is the system that supports the activities of the VA's Office of Employment Discrimination Complaint Adjudication (OEDCA), and required reporting. Cases are generated from matters brought to OEDCA for consideration, review and decision. The system is hosted in the Capital Region Readiness Center (CRRC), VA Central Office (VACO) Operations environment. The system includes custom developed applications and databases that allow OEDCA to perform legal workload management and administration of activities associated with it and for the purpose of record management for cases to be adjudicated. DCLAWS is a system inherited from the General Counsel Legal Automated Workload System (GCLAWS), with customizations to support OEDCA.

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

DCLAWS is VA-owned and operated.

2. Information Collection and Sharing

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

DCLAWS stores minimal information on approximately 100,000 employees, applicants, or former employees who have filed a formal Equal Employment Opportunity (EEO) complaint.

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

DCLAWS stores minimal contact information, dates, and case matter data for tracking information and case management. No data is shared through DCLAWS or its components.

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

The DCLAWS system operates with one web site and one database server host. The system is hosted in the Capital Region Readiness Center (CRRC), VA Central Office (VACO) Operations environment and has one web server (ogccoweb1), one application programming interface (API)/application server (ogccoapp1), and one SQL (database) server (oitcosqldclaw).

3. Legal Authority and SORN

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

The legal authority to operate the system is 38 U.S.C. 319(a)(3); (d)(2), Office of Employment Complaint Discrimination Adjudication.

H. 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 system does not have or require a SORN.

4. System Changes

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

Completion of this PIA will not result in circumstances requiring changes to the business processes.

J. Will the completion of this PIA could potentially result in technology changes?

Completion of this PIA will not result in technology changes.

Section 1. Characterization of the Information

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

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

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

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

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

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

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

Other PII/PHI data elements:

- Case Number is collected.
- If represented, Representative's Name and Email Address.
- Agency Counsel's Name
- DCLAWS does not collect, retain or share this information; however, it will keep track of the dates of these documents (these are documents received or prepared by OEDCA via email or other systems):
    - Final Agency Decision
    - Final Order
    - Remand
    - Appeal
    - U.S. Equal Employment Opportunity Commission (EEOC) Appeal Decision
    - General Correspondence
    - Deputy Secretary Package
    - Report of Investigation (ROI)
    - Administrative Judge (AJ) Decisions and Orders
    - Motions (no dates used but documents are reviewed by OEDCA attorneys – they are not stored or maintained in DCLAWS)

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

- Pleadings (no dates used but documents are reviewed by OEDCA attorneys – they are not stored or maintained in DCLAWS)

• Response Briefs
• Fee Petitions

PII Mapping of Components (Servers/Database)

DCLAWS consists of **four** key components (servers/databases/instances/applications/software/application programming interfaces (API). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by **DCLAWS** and the reasons for the collection of the PII are in the table below.

Note: Due to the PIA being a public facing document, please do not include server names in the table. The first table of 3.9 in the PTA should be used to answer this question.

Internal Components Table

Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
DCLAWS (OEDCA)	Yes	Yes	No data is shared with other systems; however, this system will maintain: • Complainant's Name • Complainant's Address (rare/few occasions) • Complainant's Email Address • Office of Resolution Management, Diversity & Inclusion (ORMDI) Case Number • If Represented, Representative's Name • Representative Email Address	Used to identify the person associated with the complaint number and contact that individual, as necessary.	Access and permissions to the data is granted thru Personal Identity Verification (PIV)/Windows Domain Authentication

Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
DCLAWS API	Yes	Yes	No data is shared with other systems; however, this system will maintain: • Complainant's Name • Complainant's Address (rare/few occasions) • Complainant's Email Address • ORMDI Case Number • If Represented, Representative's Name • Representative Email Address	Used to identify the person associated with the complaint number and contact that individual, as necessary.	Access and permissions to the data is granted thru Personal Identity Verification (PIV)/Windows Domain Authentication

Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
DCLAWS Web Client	Yes	Yes	No data is shared with other systems; however, this system will maintain: • Complainant's Name • Complainant's Address (rare/few occasions) • Complainant's Email Address • ORMDI Case Number • If Represented, Representative's Name • Representative Email Address	Used to identify the person associated with the complaint number and contact that individual, as necessary.	Access and permissions to the data is granted thru Personal Identity Verification (PIV)/Windows Domain Authentication

Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
DCLAWS Outlook Client	Yes	Yes	No data is shared with other systems; however, this system will maintain: • Complainant's Name • Complainant's Address (rare/few occasions) • Complainant's Email Address • ORMDI Case Number • If Represented, Representative's Name • Representative Email Address	Used to identify the person associated with the complaint number and contact that individual, as necessary.	Access and permissions to the data is granted thru Personal Identity Verification (PIV)/Windows Domain Authentication

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

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

The individual is not the source of the information; ORMDI is the source of the information for DCLAWS.

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

No other sources of information are required.

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

The system does not create information, but runs reports from existing data.

1.3 How is the information collected?

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

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

OEDCA collects information manually from a database maintained by the Office of Resolution Management, Diversity and Inclusion. OEDCA manually enters the information into DCLAWS.

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

OEDCA staff and DCLAWS do not collect information via a form.

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

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

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

OEDCA checks information for accuracy quarterly by running and reviewing reports.

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

The system does not check for accuracy by accessing a commercial aggregator of information.

1.5 What specific legal authorities, arrangements, and agreements defined the collection of information?

List the full legal authority for operating the system, specifically the authority to collect the information listed in question 1.1. Provide the authorities in a manner understandable to any potential reader, i.e., do not simply provide a legal citation; use statute names or regulations in addition to citations. Legal authorities include Federal laws, regulations, statutes, and Executive Orders. This question is related to privacy control AP-1, Authority to Collect

38 U.S.C. 319(a)(3); (d)(2), Office of Employment Complaint Discrimination Adjudication

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

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

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

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: OEDCA and DCLAWS stores minimal privacy information with minimal risk to any complainant. The minimal information stored within DCLAWS is required for identifying the individual associated with the complaint number and contacting that individual, if necessary. There is little to no privacy risk.

Mitigation: DCLAWS mitigates any risk by retaining only the minimal information required to identify the individual associated with the complainant and contact that individual, if necessary.

Section 2. Uses of the Information

The following questions are intended to clearly delineate the use of information and the accuracy of the data being used.

2.1 Describe how the information in the system that will be used in support of the program's business purpose.

Identify and list each use (both internal and external to VA) of the information collected or maintained. This question is related to privacy control AP-2, Purpose Specification.

PII/PHI Data Element	Internal Use	External Use
Name	Used as an identifier	Used as an identifier
Mailing Address	Used as an identifier and if correspondence needs to be sent to the Complainant	Used as an identifier and if correspondence needs to be sent to the Complainant

PII/PHI Data Element	Internal Use	External Use
Email Address	Used as an identifier	Used as an identifier
Case Number	Used as an identifier	Used as an identifier
If represented, Representative's Name	Used as an identifier	Used as an identifier
If represented, Representative's Email Address	Used as possible contact information	Used as possible contact information
Date of Final Agency Decision	Tracking date of dispatch	None
Date of Remand	Tracking date of dispatch	None
Date of Appeal	Tracking date of dispatch	None
Date of U.S. Equal Employment Opportunity Commission (EEOC) Appeal Decision	Tracking date of receipt	None
Date of General Correspondence	Tracking date of receipt	None
Date of Deputy Secretary Package	Tracking date of issuance	None
Date of Report of Investigation (ROI)	Tracking date of receipt	None
Date of Administrative Judge (AJ) Decisions and Orders	Tracking date of receipt	None
Date of Motions (no dates used but documents are reviewed by OEDCA attorneys – they are not stored or maintained in DCLAWS)	Tracking date of receipt	None
Date of Pleadings (no dates used but documents are reviewed by OEDCA attorneys – they are not stored or maintained in DCLAWS)	Tracking date of receipt	None
Date of Response Briefs	Tracking date of receipt	None
Date of Fee Petitions	Tracking date of receipt	None

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

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

Software is written in house and accessed by authorized users to analyze data using SQL queries and MS Visual Studio.

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

DCLAWS does not create any new or previously unutilized data. No data is placed in the individual's existing record. No new record will be created. No action will be taken against any individual based on the information in DCLAWS.

2.3 How is the information in the system secured?

These questions are related to security and privacy controls SC-9, Transmission Confidentiality, and SC-28, Protection of Information at Rest.

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

When the application runs within a user's web browser, all data is encrypted in transit using hypertext transfer protocol secure (HTTPS), which is the primary method to transfer data between a web browser and a web site. At the middle tier, the communications between web site and database is secured using Windows Authentication with the database source; this removes any username or password credentials stored within the connection configuration information. Connection configuration information is not embedded within the application code, rather it's stored in secured configuration files outside the application. Connection String information that is stored within the database are secured only to trusted users. Although there are several methods for securing the middle data access layer, Secure Socket Layer (SSL) encryption is not currently enabled at this level due to the impact on application performance; however, it can be enabled at any time. At the data storage level, the OEDCA database is encrypted using Transparent Data Encryption (TDE) at the file level when the data is at rest. McAfee Endpoint security is on the database servers to protect from network and file share threats.

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

The system does not collect, process, or retain Social Security Numbers.

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

DCLAWS uses VA's Governance, Risk and Compliance (GRC) tool, eMASS, to ensure all administrative, technical and physical safeguards are in place and reviewed in accordance with Government policy and standards. All OEDCA employees are required to complete VA Privacy and Information Security Awareness training and sign a Rules of Behavior annually as part of these safeguards.

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information.

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

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

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

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

2.4a How is access to the PII determined?

OEDCA managers and their proxies request access for new users by submitting a help ticket via yourIT and the template they use for this request instructs them to be specific about the type of access (basic or administrative) the new user needs. Authorized users, OEDCA attorneys and support staff are granted access on a need-to-know basis and as necessary for their job duties, as determined by documented standard operating procedures. As a minor system inheriting compliance from its major system, GCLAWS, DCLAWS will adopt and use GCLAWS SOPs.

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

Yes, DCLAWS, as a minor system inheriting compliance from its major system, GCLAWS, will adopt and use GCLAWS SOPs.

2.4c Does access require manager approval?

Yes. Manager approval is implicit with the manager's or manager proxy's request for access.

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

Access is monitored for all users through access control logs and application logs.

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

All OEDCA employees and DCLAWS authorized users are responsible for safeguarding PII. Additionally, users are required to sign the Rules of Behavior annually. The ISO is responsible for assuring that all proper measures are taken to ensure confidentiality of PII on all systems for which they are responsible.

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*

Name, Mailing Address, Email Address, Case Number

3.2 How long is information retained?

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

DCLAWS does not constitute a system of records; therefore, retention and destruction schedules do not apply.

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

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

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

DCLAWS does not constitute a system of records.

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

DCLAWS does not constitute a system of records.

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

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

Through DCLAWS, no records are destroyed, eliminated or transferred to NARA.

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

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

PII is not used for research, testing or training.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

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

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

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

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

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

Follow the format below:

Privacy Risk: If data is disclosed to unauthorized individuals, it would have only a limited adverse impact on VA operations, assets, or individuals.

Mitigation: DCLAWS mitigates this risk by retaining only minimal PII.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

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

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

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

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

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

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

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system***	***Describe the method of transmittal***
Veterans Benefits Administration	To inform or advise that a decision has been issued	Sent: Final Agency Decision, Final Order, Remand, Complainant's name/ORMDI case number, Complainant's email address (if there is a Representative, Representative email address), Appeals	Microsoft Outlook Email (no data is shared through DCLAWS with this organization)
Veterans Health Administration	To inform or advise that a decision has been issued.	Sent: Final Agency Decision, Final Order, Remand, Complainant's name/ORMDI case number, Complainant's email address (if there is a Representative, Representative email address), Appeals	Microsoft Outlook Email (no data is shared through DCLAWS with this organization)

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system***	***Describe the method of transmittal***
Office of Resolution Management, Diversity & Inclusion (ORMDI)	To request a supplemental investigation and/or to obtain more information regarding a case or to inform or advise that a decision has been issued.	Sent: Final Agency Decision, Final Order, Remand, Complainant's name/ORMDI case number, Complainant's email address (if there is a Representative, Representative email address), Appeals, AJ/EEOC Decisions	Microsoft Outlook Email (no data is shared through DCLAWS with this organization)
Office of Resolution Management, Diversity & Inclusion (ORMDI) E2	To gather information necessary to adjudicate formal EEO complaints.	Accessed and/or Received: Complainant's name/case number, Complainant's email address (occasionally home address), if Represented, Complainant's Representative's name and email address, Agency counsel's name and email, General Correspondence Accessed only: Reports of Investigation, AJ Decisions	Microsoft Outlook Email, Microsoft Dynamics 365 E2 web portal (Please note that we can access this data in a read-only format even though it is not shared with DCLAWS and we do not enter any data into E2.)
Office of the Secretary of Veterans Affairs	To inform or advise that a decision has been issued.	Sent: Final Agency Decision, Final Order, Remand, Deputy Secretary's Package, Complainant's name/ORMDI case number, Complainant's email address (if there is a Representative, Representative email address), Appeals	Microsoft Outlook Email, VA Integrated Enterprise Workflow Solution (VIEWS)

List the Program Office or IT System information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT system*	*List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system*	*Describe the method of transmittal*
Office of Policy and Compliance	To inform or advise that a decision has been issued and to request monitoring compliance with OEDCA orders.	Sent: Final Agency Decision, Final Order, Remand, Complainant's name/ORMDI case number, Complainant's email address (if there is a Representative, Representative email address), Appeals Sent and Received: EEOC Decisions, AJ Decisions, and General Correspondence	Microsoft Outlook Email (no data is shared through DCLAWS with this organization)
National Cemetery Administration	To inform or advise that a decision has been issued.	Sent: Final Agency Decision, Final Order, Remand, Complainant's name/ORMDI case number, Complainant's email address (if there is a Representative, Representative email address), Appeals	Microsoft Outlook Email (no data is shared through DCLAWS with this organization)
VA Central Office/Other Staffing Offices	To inform or advise that a decision has been issued.	Sent: Final Agency Decision, Final Order, Remand, Complainant's name/ORMDI case number, Complainant's email address (if there is a Representative, Representative email address), Appeals	Microsoft Outlook Email, (no data is shared through DCLAWS with this organization)
Complaints Automated Tracking System (CATS)	To gather information necessary to adjudicate formal EEO complaints.	Accessed and/or Received: Complainant's name/case number, Complainant's email address (occasionally home address), if Represented, Complainant's Representative's name and email address, Agency counsel's name and email, General Correspondence, Reports of Investigation, AJ Decisions	CATS Portal (We do not share any data (including PII data) with CATS and neither will DCLAWS. We only have read-only access.)

4.2 <u>PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure</u>

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

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

Follow the format below:

Privacy Risk: If data is disclosed to unauthorized individuals, it would have only a limited adverse impact on VA operations, assets, or individuals.

Mitigation: DCLAWS mitigates this risk by retaining only minimal PII.

Section 5. External Sharing/Receiving and Disclosure

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

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

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

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

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

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

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

Describe how the information is transmitted to entities external to VA and what security measures have been taken to protect it during transmission.
This question is related to privacy control UL-2, Information Sharing with Third Parties

Data Shared with External Organizations

List External Program Office or IT System information is shared/received with	***List the purpose of information being shared / received / transmitted with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program or IT system***	***List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)***	***List the method of transmission and the measures in place to secure data***
U.S. Equal Employment Opportunity Commission (EEOC) Federal Sector EEO Portal (FedSEP)	To gather information necessary to adjudicate formal EEO complaints.	Accessed/Received: Complainant's name/case number, Complainant's email address, phone number, Representative's email address/mailing address/phone number, Complainant's home address, agency counsel, Report of Investigation (ROI), Administrative Judge (AJ) Decisions, correspondence, motions, pleadings, and orders from the AJ	We do not have an agreement because we do not share any information with them now (nor will we using DCLAWS). We can access their records through a read-only web portal. That portal contains documents filed in the case as part of the litigation. It is not, and will not, be connected to DCLAWS. DCLAWS will not receive information from it.	Microsoft Outlook Email (only receive alerts with no specific case details or copies of AJ Decisions and Orders), Federal Sector EEO Portal (FedSEP)

List External Program Office or IT System information is shared/received with	***List the purpose of information being shared / received / transmitted with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program or IT system***	***List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)***	***List the method of transmission and the measures in place to secure data***
Complainant's Representatives (which may include law firms)	To inform or advise that a decision has been issued.	May Receive: Complainant's name/case number, Complainant's email address, Representative's email address, home address, agency counsel, responses to investigative reports, fee petitions	We do not have an agreement because we do not share any information with them now (nor will we using DCLAWS). We only email them a copy of the final decision in a case and they send us responses to investigations conducted or fee petitions.	Microsoft Outlook Email

List External Program Office or IT System information is shared/received with	***List the purpose of information being shared / received / transmitted with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program or IT system***	***List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)***	***List the method of transmission and the measures in place to secure data***
Complainant	To inform or advise that a decision has been issued.	Complainant's name/case number, Complainant's email address, home address, agency counsel, responses to investigative reports, fee petitions	We do not have an agreement because we do not share any information with them now (nor will we using DCLAWS). We only email them a copy of the final decision in a case and they send us responses to investigations conducted or fee petitions.	Microsoft Outlook Email

5.2 <u>PRIVACY IMPACT ASSESSMENT: External sharing and disclosure</u>

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

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

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

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

Follow the format below:

Privacy Risk: If data is disclosed to unauthorized individuals, it would have only a limited adverse impact on VA operations, assets, or individuals.

Mitigation: DCLAWS mitigates this risk by manually entering data obtained from external sources and by issuing decisions to external organizations through MS Outlook. No PII is shared through DCLAWS.

Section 6. Notice

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

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

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

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

DCLAWS does not collect any information from the individual. (The Office of Resolution Management, Diversity and Inclusion receives the information directly from the individual and enters it into its database, where OEDCA staff use read-only access to retrieve the information and enter it manually into DCLAWS.)

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

DCLAWS does not collect any information from the individual.

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

DCLAWS does not collect any information from the individual.

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.

DCLAWS does not collect any information from the individual.

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.

DCLAWS does not collect any information from the individual.

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. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

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

Principle of 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: DCLAWS does not collect any information from the individual.

Mitigation: DCLAWS does not collect any information from the individual.

Section 7. Access, Redress, and Correction

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

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

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

7.1a Cite any procedures or regulations your program has in place that allow access to information. These procedures, at a minimum, should include the agency's FOIA/Privacy Act practices, but may also include additional access provisions. ***For example, if your program has a customer satisfaction unit, that information, along with phone and email contact information, should be***

listed in this section in addition to the agency's procedures. See 5 CFR 294 and the VA FOIA Web page at http://www.foia.va.gov/ to obtain information about FOIA points of contact and information about agency FOIA processes.

OEDCA does not process first-party or third-party Privacy Requests. ORMDI is the official records keeper.

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

ORMDI is the official records keeper.

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

ORMDI is the official records keeper.

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.

Requests for data correction can be made ORMDI by email to one of its regional offices:

Region	Email
20DR-NAD 2	lakiaha.haskins@va.gov
2003-Continental District	ORMContinentalDistrictFrontOffice@va.gov
2004-NAD 2	ORMNAD2FrontOffice@va.gov
200H-NAD 1	ORMNEOAdministrativeGroup@va.gov
200I-Southeastern District	ORMSEDCORRESPONDENCE@va.gov
200J-Midwest District	ORMMDFrontOffice@va.gov
200P-Pacific District	ORMpacificdistrict@va.gov

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.

Requests for procedures for correcting data can be made by email to ORMDI.

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

Redress is the process by which an individual gains access to his or her records and seeks corrections or amendments to those records. Redress may be provided through the Privacy Act and

Freedom of Information Act (FOIA), and also by other processes specific to a program, system, or group of systems. ***Example: Some projects allow users to directly access and correct/update their information online. This helps ensures data accuracy.***
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Requests for redress can be made by email to ORMDI.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

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

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

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

Follow the format below:

Privacy Risk: There are no options for access, redress, or correction through DCLAWS because ORMDI is the official records keeper.

Mitigation: There are no options for access, redress, or correction through DCLAWS because ORMDI is the official records keeper.

Section 8. Technical Access and Security

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

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

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

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

Procedures for setting up users with access are documented via Standard Operating Procedures (SOPs). Managers are instructed to input a yourIT ticket and provide the date the user

signed the Rules of Behavior. Managers are also instructed to specify exactly what type of access the new employee requires.

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

Users from other agencies do not have access to the system.

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

The system is designed to allow only authorized users, OEDCA attorneys and support staff, access on a need-to-know basis and can be made available to any OEDCA employee as necessary. Database roles are assigned to users where selected administrator staff and supervisors are granted full access, while other employees including attorneys are granted limited access, mainly read-only access.

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.

Contractors will not have access to sensitive information in the production environment. However, contractors will have access to lower environments, which do not have sensitive information. Contractors must acknowledge awareness of security practices via annual VA Privacy Security Awareness (PISA) and Rules of Behavior training certifications.

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.

OEDCA Talent Management System (TMS) administrators and the ISO use the VA TMS for tracking all training records. All OEDCA users are required to take Information Security Awareness and Privacy Act Training and those records are maintained by employees, supervisors, and management. Management reviews the status of training requirements and track progress. The VA Office of Human Resources is responsible for maintaining security and privacy awareness training records for each employee. Also, the system-use notification message

provides appropriate privacy and security notices (based on associated privacy and security policies or summaries) and remains on the screen of each application until the user takes explicit actions to log on to the information system. OEDCA also provides training, not captured in TMS, to its staff regarding the sensitivity of the records contained in DCLAWS.

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

No.

8.4a If Yes, provide:

1. *The Security Plan Status:* <<ADD ANSWER HERE>>
2. *The System Security Plan Status Date:* <<ADD ANSWER HERE>>
3. *The Authorization Status:* <<ADD ANSWER HERE>>
4. *The Authorization Date:* <<ADD ANSWER HERE>>
5. *The Authorization Termination Date:* <<ADD ANSWER HERE>>
6. *The Risk Review Completion Date:* <<ADD ANSWER HERE>>
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* Moderate

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

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

The A&A is in progress with an IOC date estimated at 05/1/2024.

Section 9 – Technology Usage

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

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

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

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

DCLAWS does not use cloud technology.

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

DCLAWS does not use cloud technology.

9.3 Will the CSP collect any ancillary data and if so, who has ownership over the ancillary data?

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

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

DCLAWS does not use cloud technology.

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

What are the roles and responsibilities involved between the organization and cloud provider, particularly with respect to managing risks and ensuring organizational requirements are met? This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.

DCLAWS does not use cloud technology.

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

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

DCLAWS does not use cloud technology.

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

Signature of Responsible Officials

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

TAYLOR BANKS

Digitally signed by TAYLOR BANKS
Date: 2024.02.15 10:54:22 -06'00'

Privacy Officer, Taylor S. Banks

KENEATH COLEMAN

Digitally signed by KENEATH COLEMAN
Date: 2024.02.16 07:57:28 -05'00'

Information System Security Officer, Keneath Coleman

KALPANA RAMIREDDY

Digitally signed by KALPANA RAMIREDDY
Date: 2024.02.15 15:42:16 -05'00'

Information System Owner, Kalpana Ramireddy

APPENDIX A-6.1

Please provide a link to the notice or verbiage referred to in Section 6 (a notice may include a posted privacy policy; a Privacy Act notice on forms; screen shot of a website collection privacy notice).

HELPFUL LINKS:

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

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

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

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

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