



U.S. DEPARTMENT OF LABOR

**Veterans' Employment and
Training Service (VETS)**



**VETS CASE MANAGEMENT
SYSTEM (VCMS)**

PRIVACY IMPACT ASSESSMENT

VERSION 1.4

1/8/2024

DOCUMENT CHANGE HISTORY

Date	Filename / Version #	Author	Revision Description
4/4/19	VCMS PIA / Version 1.0	Appteon Inc.	Initial
4/15/19	VCMS PIA/ Version 1.1	Appteon Inc.	Modifications to Sections 1.8 and 1.9
04/08/20	VCMS PIA/ Version 1.2	Collabralink Inc.	Annual review/updates
02/24/21	VCMS PIA/Version 1.3	VCMS Support Team	Annual review/updates
01/8/24	VCMS PIA/Version 1.4	VCMS Support Team	Annual review/updates

DOCUMENT REVIEW HISTORY

Date	Version #	Reviewers
1/5/2021	1.3	Chantel A. Ford
1/8/2024	1.4	Kris Evans, Tom Carl, Arti Bhagwat

TABLE OF CONTENTS

Privacy Impact Assessment Questionnaire	4
1.1 Overview	4
1.2 Characterization of the Information	4
1.3 Describe the Uses of the PII.....	7
1.4 Retention	9
1.5 Internal Sharing and Disclosure	11
1.6 External Sharing and Disclosure	13
1.7 Notice	15
1.8 Individual Access, Redress, and Correction.....	16
1.9 Technical Access and Security.....	17
1.10 Technology.....	19
1.11 Determination.....	20
1.12 PIA Signature Page	21
Appendix A: Definitions for PII and PII Elements this System Collects.....	22

PRIVACY IMPACT ASSESSMENT QUESTIONNAIRE

OVERVIEW

The Veterans' Employment and Training Service (VETS) Case Management System (VCMS) is a digital solution which allows for the submission of complaints filed by claimants alleging violations of the Uniformed Services Employment and Reemployment Rights Act (USERRA) and the laws and regulations relating to veterans' preference (VP) in Federal employment, including the Veterans Employment Opportunities Act (VEOA), and the processing and management of those cases. The VCMS is a part of an ongoing initiative to modernize the current processes and procedures used to investigate complaints filed with VETS. The VCMS is a web-based application built on Appian, hosted on the AWS GovCloud environment.

AWS GovCloud (US) is an AWS region designed to allow United States (U.S.) government agencies at the federal, state, and local level, along with contractors, educational institutions and other U.S. customers to run sensitive workloads in the cloud by addressing their specific regulatory and compliance requirements. Beyond the assurance programs applicable to all AWS regions, the AWS GovCloud (US) region allows customers to adhere to Federal Risk and Authorization Management Program (FedRAMP) requirements.

CHARACTERIZATION OF THE INFORMATION

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

Specify whether the System collects personally identifiable information (PII) on Department of Labor (DOL) employees, other federal employees, contractors, members of the public (U.S. citizens), foreign citizens, or minor children.

The VCMS collects information of VETS federal employees, and members of the public, including claimants, witnesses, employers, and other individuals who have personal knowledge within the scope of USERRA or VP investigations. These members of the public include U.S. citizens, and, in some cases, foreign citizens. Claimant, witness, and employer information is stored on an Oracle Database on the AWS GovCloud environment. Generated documents related to each case are stored and maintained on SharePoint at <https://usdol.sharepoint.com/sites/cmpvetsvcms>. Case access within the VCMS is restricted to authorized system users assigned to each case, and privileged users who maintain the system.

- From whom is information to be collected?

Members of the public, including claimants, witnesses, employers, and other individuals with personal knowledge within the scope of USERRA and VP investigations.

- Why is the information being collected?

In accordance with 38 U.S.C. § 4322 and 5 U.S.C. § 3330a, VETS is charged with conducting investigations into all USERRA and VP claims submitted in writing to the Agency. The investigation of such claims requires the collection and retention of information about the

claimants submitting such claims, the witnesses to the facts and circumstances alleged in such claims, employers who are the subject of such claims, and other individuals with personal knowledge of the facts and circumstances directly or indirectly related to such claims.

- What is the PII being collected, used, disseminated, or maintained?

The PII that is collected as a part of the investigative process may include:

- Names
 - Addresses
 - Phone Numbers
 - Email Addresses
 - Date of Birth
 - Social Security Numbers
 - Sex/Gender
 - Race/Ethnicity
 - Medical History
 - Disability Status
 - Compensable Disability Financial Information
 - Pension Information
 - Salaries, Payroll Data, and Wage Records
 - Tax Records
 - Credit History
 - Applicant and Employee Hiring, and Termination Data
 - Employee Performance Data and Reports
 - Military Service Record Information
 - Employment and Educational Information
 - Criminal Background Information
 - Powers of Attorney
 - Telephone and other Communication Records
- How is the PII collected?
- PII for claims filed with VETS is collected initially through the claim filing process on the VETS/USERRA/VP Data Eligibility Form 1010 (OMB No. 1293-0002) (VETS 1010). Additional PII is collected throughout each investigation, if determined necessary by the assigned investigator to evaluate the merits of each issue raised in the subject case. PII may be received in hard copy by mail, or fax, or in soft copy through email, direct submission in the VCMS, or received verbally from persons related to the investigations through in-person, video, or telephonic communication. Information received verbally is entered by investigators on a VETS Form 1063, Report of Contact, inside the VCMS.
- How will the information collected from individuals or derived from the system be checked for accuracy?

Collected information and data are primarily validated by the assigned investigator for each case. The work of each investigator is reviewed routinely throughout and at the conclusion of each investigation by supervisors and/or designated reviewers. Finalized data within the system is reviewed quarterly and annually by VETS Senior Compliance Analyst, and the

VETS Compliance Data Center (VCDC) team.

- What specific legal authorities, arrangements, and/or agreements defined allow the collection of PII?

USERRA authorizes the Secretary of Labor (“the Secretary”), through VETS, to provide assistance to any person or entity regarding the employment and reemployment rights and benefits provided under the statute, including any Federal employee or applicant who requests it. *See* 38 U.S.C. § 4321, 5 C.F.R. § 353.210, and 20 C.F.R. §§ 1002.4 & 1002.277.

USERRA provides that a person who claims that he or she is entitled to employment or reemployment rights or benefits under USERRA with respect to employment by an employer, including a Federal executive agency, and such employer has failed or refused, or is about to fail or refuse, to comply with the provisions of USERRA, that person may file a complaint with the Secretary, and the Secretary shall investigate such complaint. *See* 38 U.S.C. § 4322(a) and 20 C.F.R. § 1002.288.

In carrying out any investigation under USERRA, the Secretary’s duly authorized representatives shall, at all reasonable times, have reasonable access to and the right to interview persons with information relevant to the investigation and shall have reasonable access to, for the purposes of examination, and the right to copy and receive, any documents of any person or employer that the Secretary considers relevant to the investigation. *See* 38 U.S.C. § 4326(a) and 20 C.F.R. § 1002.289.

The Secretary's responsibilities under VP are codified at 5 U.S.C. § 3330a, and those responsibilities have been delegated to VETS by the Secretary. A preference eligible individual in a federal employment action who alleges a violation of VP rights by an agency, or a veteran who alleges that an agency has violated the VEOA in Federal employment, may file a complaint with VETS. *See* 5 U.S.C. § 2108(3), 5 U.S.C. § 3304(f)(1), and 5 U.S.C. § 3330a(a)(1).

Under the VEOA, VETS is responsible for providing technical assistance to potential complainants upon request; investigating complaints during which VETS can issue administrative subpoenas, as necessary, to conduct investigations; and making reasonable efforts to resolve meritorious complaints. *See* 5 U.S.C. § 3330a(a)(3), 5 U.S.C. § 3330a(b), and 5 U.S.C. § 3330a(c).

- Privacy Impact Analysis

The identified risks are directly related to the collection and use of the PII by authorized individuals or entities. Access to case data is consistent with DOL Cybersecurity Policy Portfolio (CPP) requirements for access control and separation of duties.

Possible risks include the following:

1. Inappropriate use of the PII collected;
2. Failure to secure any hardcopy documents on which PII appears.
3. Malicious theft of data by a motivated outside attacker.

The mitigation actions that are currently employed to reduce the potential of exposure of the

identified PII are the following:

1. Establish and provide secure access to the VCMS;
2. Conduct departmental annual training to all DOL employees and contractors on Cybersecurity and Privacy Awareness;
3. Provide access to and training for the proper disposal (shredding and/or burning) of all hardcopy documents prior to disposal and/or for the destruction of all electronic portable media (CDs, USB Drives, Memory Cards, etc.) received or used during the investigation and evaluation processes conducted through the VCMS, including the acquisition and use of shredding devices at all VCMS office locations;
4. Minimize all data collection to the minimum necessary to conduct investigations;
5. Enforce rigorous protection standards to ensure accuracy and confidentiality when shipping or mailing documents.
6. Restrict available roles for each user based on their business needs and their assigned geographic jurisdiction.

DESCRIBE THE USES OF THE PII

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

- Describe all the uses of the PII

PII is used by VETS staff in investigating USERRA and VP cases. PII is required at initial claim intake to establish the identity and eligibility of a claimant requesting assistance. PII is also requested and obtained to establish sufficient facts and information to determine whether a case has been substantiated by the evidence and found to have or lack merit. In a case determined to be meritorious, or in which a claimant or employer wishes to pursue a settlement, PII may be used to determine the appropriate remedies due to a claimant.

Demographic PII may also be separated from unique identifiers, and used in reporting to determine fair and equal treatment of demographic groups filing claims with VETS.

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

Microsoft products (Excel, Access), Tableau, SQL Developer, and other developer tools are used to produce aggregate statistical results.

- Will the system derive new data, or create previously unavailable data, about an individual through aggregation of the collected information?

No.

- If the system uses commercial or publicly available data, please explain why and how it is used.

Publicly available data is used as follows:

1. Melissa for address validation;

2. Standard Occupational Classification System Codes (SOCS Codes) to determine the industry-type for claimant's civilian employment position;
 3. The 13-week Treasury Bill interest rates to determine applicable interest due for back wage computations and pension benefit calculations.
- Will the use of PII create or modify a "system of records notification" under the Privacy Act?

Yes. This is managed under the existing VCMS System of Records Notification, DOL/VETS-6.

- Privacy Impact Analysis

In order to comply with the departmental requirements, VCMS privileged users and administrators will:

1. Conduct monthly audit log and account reviews;
2. Conduct bi-annual account recertifications;
3. Annually renew Rules of Behavior (ROB) for all users;
4. Dividing mission functions and information system support functions among different individuals and/or roles;
5. Conducting information system support functions with different individuals (e.g., system management, programming, configuration management, quality assurance and testing, and network security);
6. Ensuring security personnel administering access control functions do not also administer audit functions; or
7. Different administrator accounts exist and are used for different roles;
8. Prevent non-privileged users from executing privileged functions;
9. Employ the principle of least privilege, allowing only authorized accesses for users that are necessary to accomplish assigned organizational tasks.

Retention

The following questions are intended to outline how long information will be retained after the initial collection.

- What is the retention period for the data in the system?

Records are retained until litigation is completed, then transferred to the National Archives and Records Administration (NARA) Federal Records Center two years after cutoff. Records are destroyed when they are ten years old, except for USERRA case files involving pension benefits in which claimants were not in retired status from civilian employment at the time of cutoff, which will be retained for fifty years after cutoff pursuant to N1-174-88-1 and Veterans' Employment and Training Service Director's Memorandum 1-01 (Change-1). Electronic case management information is retained indefinitely. A physical date does not apply as there are multiple periods of retention for the various data sets collected in the

systems.

- Is a retention period established to minimize privacy risk?

Retention is currently indefinite, subject to an updated retention schedule request submitted to NARA.

- Has the retention schedule been approved National Archives and Records Administration (NARA)?

VCMS has used an approved retention schedule for electronic records/case files pursuant to N1-174-88-1, approved on February 8, 1988, and N1-174-90-2, approved on February 9, 1990. An updated Electronic Information System (EIS) Request was submitted for approval on February 21, 2021. This PIA will be reviewed and updated following the approval of the request.

- Per M-17-12, *Preparing for and Responding to the Breach of Personally Identifiable Information*; what efforts are being made to eliminate or reduce PII that is collected, stored or maintained by the system if it is no longer required?

USERRA and VP investigation data requirements have been reviewed by Agency management and determined to be necessary to meet statutory obligations where no statute of limitations is applicable. Specifically, the Veterans' Benefit and Improvement Act of 2008 (VBIA), in pertinent part, implemented reforms to the USERRA complaint process, including no time limit on the period for filing a USERRA complaint or claim with the Secretary, before the Merit Systems Protection Board (MSPB), or a Federal or State court. Pub.L. No. 110-389 § 311, 38 U.S.C. § 4327(b).

- Have you implemented the DOL PII Data Extract Guide for the purpose of eliminating or reducing PII?

Not applicable; the VCMS does not create PII data extracts.

- How is it determined that PII is no longer required?

While the agency exports and relinquishes all hard copy data in accordance with its NARA record schedule, all electronic data is retained indefinitely to comply with the Agency's statutory obligations under USERRA where no statute of limitations is applicable. Specifically, the VBIA, in pertinent part, implemented reforms to the USERRA complaint process, including no time limit on the period for filing a USERRA complaint or claim with the Secretary, before the MSPB, or a Federal or State court. Pub.L. No. 110-389 § 311, 38 U.S.C. § 4327(b).

- If you are unable to eliminate PII from this system, what efforts are you undertaking to mask, de-identify or anonymize PII.

Record access within the VCMS is curtailed to only staff who require access to individual USERRA and VP case records as part of the investigative or review process. Privileged user groups have access to all system data; however, all data exports contain masked Social Security Numbers. PII contained within case documents in the system are not included in

any data export and are only included as a component of NARA and Freedom of Information Act (FOIA) packages. All FOIA packages are thoroughly reviewed by FOIA coordinators who mask or redact all PII prior to transmission in accordance with FOIA.

- Privacy Impact Analysis

VETS staff members and system administrators will:

1. Enforce records disposition instructions to manage a records lifecycle;
2. Prevent unauthorized access, alteration, concealment, or destruction of records;
3. Review and redact privileged and protected information from disclosure when preparing documents and materials in response to a Freedom of Information request or request under the Privacy Act.

INTERNAL SHARING AND DISCLOSURE

The following questions are intended to define the scope of sharing within the Department of Labor.

- With which internal organization(s) is the PII shared, what information is shared, and for what purpose?

PII is shared with the DOL's Office of the Solicitor (SOL) attorneys, who assist in reviewing and providing legal advice and counsel to investigators during the course of investigations.

- How is the PII transmitted or disclosed?

PII is transmitted to VETS investigators by mail, fax, email, and the VCMS upload feature, and verbally in person, by phone, or through video conferencing. PII contained within case files is accessible by VETS users assigned to investigate and review cases, and SOL attorneys when consultation is requested.

- Does the agency review when the sharing of PII is no longer required to stop the transfer of sensitive information?

Not applicable; the information is maintained in the VCMS to support NARA records retention and FOIA disclosure requirements, and potential future re-opened USERRA investigations and referral actions of USERRA cases to DOJ and OSC where no statute of limitations is applicable.

- Privacy Impact Analysis

VCMS privileged users and administrators will protect privileged information accessible by internal users by enforcing system rules of behavior and account roles assignments based on separation of duties and principles of least privileges. Administrators will review existing internal accounts on a regular basis and remove any roles or system access that are not required for a user to complete business functions within their assigned geographical jurisdiction.

EXTERNAL SHARING AND DISCLOSURE

The following questions are intended to define the content, scope, and authority for information sharing external to DOL which includes federal, state, and local government, and the private sector.

- With which external organization(s) is the PII shared, what information is shared, and for what purpose?

PII contained within USERRA case files is transferred to DOJ or OSC following a written request by claimants for referral to DOJ or OSC for consideration of representation and litigation in accordance with USERRA. PII contained within VP case files is transferred to OSC pursuant to the Department's Memorandum of Understanding (MOU) with OSC to refer meritorious complaints to OSC as potential prohibited personnel practices. DOJ and OSC case file access is limited to data required to consider and pursue litigation in support of USERRA and VP enforcement activities. *See* 38 U.S.C. §§ 4323 and 4324, and 5 U.S.C. §§ 1214 and 2302(b)(11)

- Is the sharing of PII outside the Department compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If so, please describe. If not, please describe under what legal mechanism the program or system is allowed to share the PII outside of DOL.

VETS shares PII outside the Department with DOJ and OSC under USERRA and the laws and regulations relating to VP in Federal hiring. PII contained within USERRA case files is shared with DOJ or OSC following a written request by claimants for referral to DOJ or OSC for consideration of representation and litigation in accordance with USERRA. PII contained within VP case files is shared with OSC pursuant to the Department's MOU with OSC to refer meritorious complaints to OSC as potential prohibited personnel practices. DOJ and OSC case file access is limited to data required to consider and pursue litigation in support of USERRA and VP enforcement activities. *See* 38 U.S.C. §§ 4323 and 4324, and 5 U.S.C. §§ 1214 and 2302(b)(11).

- How is the information shared outside the Department and what security measures safeguard its transmission?

USERRA and VP case file data is transferred to DOJ or OSC by granting access to the electronic case file within VCMS by VETS National Office program staff. DOJ and OSC users have distinct system roles that control access to only the cases that have been approved for transfer.

- How is the information transmitted or disclosed?

See above response.

- Is a Memorandum of Understanding (MOU), contract, or any agreement in place with any external organizations with whom information is shared, and does the agreement reflect the scope of the information currently shared? If yes, include who the agreement is with and the duration of the agreement.

An MOU between VETS and OSC was signed in December 2000, and an MOU between DOL and DOJ was signed on December 8, 2021; both remain in effect. PII contained within USERRA case files is shared with DOJ or OSC following a written request by claimants for referral to DOJ or OSC for consideration of representation and litigation in accordance with USERRA. PII contained within VP case files is shared with OSC pursuant to the MOU to refer meritorious complaints to OSC as potential prohibited personnel practices. DOJ and OSC case file access is limited to data required to consider and pursue litigation in support of USERRA and VP enforcement activities. *See* 38 U.S.C. §§ 4323 and 4324, and 5 U.S.C. §§ 1214 and 2302(b)(11).

- How is the shared information secured by the recipient?

Information provided to the DOJ is secured in DOJ's JEFS. JEFS is maintained by DOJ's Civil Rights Division. JEFS is compliant with OMB Circular A-130, OMB M-17-12, OMB M-16-24, DOJ Order 2640.2 (series), DOJ Order 2740.1 (series), and the DOJ Cybersecurity Standard.

Information provided to OSC is secured in compliance with OSC Directive No.153: Computer Network User Roles and Responsibilities, and OSC Directive No.155: Security of Personally Identifiable information in Electronic Form.

- What type of training is required for users from agencies outside DOL prior to receiving access to the information?

External Federal agencies are required to conduct their own internal training on the use and handling of PII on an annual basis.

- Privacy Impact Analysis

External users are required to comply with DOL system rules of behavior and are required to annually recertify that they agree to the terms and conditions contained within the rules of behavior. External accounts are audited monthly.

NOTICE

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

- Was notice provided to the individual prior to collection of PII? 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 Notice. If notice was not provided, please explain.

Yes; see Privacy Notice on the VETS 1010 Complaint Form in Appendix B. This notice states that: The primary use of this information is by staff of the Veterans' Employment and Training Service in investigating cases under USERRA or laws/regulations relating to veterans' preference in Federal employment. Disclosure of this information may be made to: a Federal, state or local agency for appropriate reasons; in connection with litigation; and to an individual or contractor performing a Federal function. Furnishing the information on this

form, including your Social Security Number, is voluntary. However, failure to provide this information may jeopardize the Department of Labor's ability to provide assistance or complete an investigation of your complaint.

- Do individuals have the opportunity and/or right to decline to provide information?

Yes; however, users are made aware that failure to provide information may jeopardize the Department's ability to provide assistance on their claims.

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

Yes; individuals submitting information to file USERRA or VP complaints are consenting to the proposed use of their PII in order to investigate their claims under USERRA or VP.

- Privacy Impact Analysis

The VETS 1010 Complaint Form (paper and online) clearly displays the Privacy Act notices for all users to read and understand their individual rights in submitting PII data.

INDIVIDUAL ACCESS, REDRESS, AND CORRECTION

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

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

Individuals may request their own information from investigators assigned to cases in which they are involved. During the course of an investigation, the investigator may provide copies of information back to the individual on request, if that information was originally provided by the individual. Claimants may also obtain access to their own data through use of the VCMS. The VCMS is an Internet-based system that allows USERRA claimants to officially submit a complaint via the VETS electronic Form 1010 (e-1010) available through <https://vets1010.dol.gov>. A claimant may gain access to his or her own information after submitting a complaint by registering for access to the VCMS, and accessing submitted data through the site. Additional information relating to the investigation, including a requestor's own information, also may be obtained through a written request in accordance with FOIA or Privacy Act.

- What are the procedures for correcting inaccurate or erroneous information?

After collecting information from individuals involved in a USERRA or VP case, the assigned investigator is responsible for correcting any inaccuracies or erroneous information contained in the case file before completing the investigation and closing the case.

- How are individuals notified of the procedures for correcting their own information?

Individuals are informed verbally by the assigned investigator conducting the investigation in which the information was collected on how to correct inaccurate or erroneous information.

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

Claimants who express disagreement with the handling of their USERRA claim, including with regard to any information collected, can file a protest with the Agency under VETS protest procedures either during the investigation or after the investigation is closed in accordance with VETS USERRA/VP/VEOA Investigations Manual, Chapter 12.3.

- Privacy Impact Analysis

The VETS 1010 Complaint Form (paper and online) clearly displays the Privacy Act notices for all users to read and understand their individual rights in submitting PII data.

TECHNICAL ACCESS AND SECURITY

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

- Which user group(s) will have access to the system? (For example, program managers, IT specialists, and analysts will have general access to the system and registered users from the public will have limited access.)

Access is limited to VETS investigators, reviewers, administrators, and contractor staff responsible for conducting and reviewing investigations, and reporting and monitoring program performance and system functionality. The system is accessible internally to SOL attorneys, who assist in reviewing and providing legal advice and counsel to investigators during the course of investigations, and externally to DOJ and OSC following a written request by claimants for referral of a USERRA case to DOJ or OSC for consideration of representation and litigation in accordance with USERRA, and to OSC pursuant to the Department's MOU with OSC to refer meritorious complaints to OSC as potential prohibited personnel practices. DOJ and OSC case file access is limited to data required to consider and pursue litigation in support of USERRA and VP enforcement activities. *See* 38 U.S.C. §§ 4323 and 4324, and 5 U.S.C. §§ 1214 and 2302(b)(11). Limited system access is also available to the claimants to submit claims and documents. Claimants access is restricted to their original submitted claim, submitted documents, and current case status.

- Will contractors to DOL have access to the system? If so, please include a copy of the contract describing their role to the OCIO Security with this PIA.

Limited access to the production system (Prod) is provided to the contractor Developer(s) on all contracts for the purpose of diagnosing system issues identified by users, but they cannot modify or extract data independently. The contractor Developer(s), Business Analyst(s), and Tester(s) assigned to any contract have full access in Dev, Dev2, Test, and Pre-Production Environments, which do not contain any PII.

- Do the system use "roles" to assign privileges to users of the system? If yes, describe the roles.

Yes; the VCMS employs role-based access. Users are assigned roles based on the functions of the system that they are required to access based on their business needs and geographic jurisdiction.

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

Access Control/Account Management procedures are consistent with DOL's CPP. Specific rules regarding which users may have individual roles are further defined in the VCMS agency user guide and in the USERRA/VP/VEOA Investigations Manual.

- How are the actual assignments of roles and Rules of Behavior, verified according to established security and auditing procedures? How often training is provided? Provide date of last training.

Roles are established and managed by the VCMS privileged user group. All users must complete the OASAM Rules of Behavior and submit a system access request prior to being granted access to the system. Requests for account access, modification, and deletion require supervisory approval, and National Office approval prior to any change. Employees participate in mandatory Privacy Act and Records Management training annually. Training completions are recorded and tracked in the Department's Learning Link System. Bi-annual account certification is conducted to ensure access is routinely reviewed. All accounts are reviewed and certified by both the Regional Administrator for field accounts within their area of responsibility and the National Office.

- Describe what privacy training is provided to users, either generally or specifically relevant to the program or system?

Employees participate in mandatory Privacy Act and Records Management training annually. Training completions are recorded and tracked in the Department's Learning Link System.

- What auditing measures and technical safeguards are in place to prevent misuse of data?

Auditing measures and other technical safeguards, such as quarterly and annual reviews of finalized data by the Senior Compliance Analyst and the VCDC, Access Control/Account Management procedures, and quarterly account certification, are provided by the VCDC staff and OCIO to prevent the misuse of data.

- Is the data secured in accordance with FISMA requirements? If yes, when was Security Assessment and Authorization last completed?

Yes; the Security Assessment and Authorization was last reviewed and edited in December 2023.

- Privacy Impact Analysis

1. User Group Access:

- The system is accessible to VETS investigators, reviewers, administrators, and contractor staff responsible for conducting and reviewing investigations, reporting, and monitoring program performance and system functionality.
- SOL attorneys have internal access to assist in reviewing and providing legal advice and counsel to investigators.
- DOJ and OSC have external access following a written request by claimants for referral of a USERRA case to DOJ or OSC for consideration of representation and litigation.

- Access for DOJ and OSC is limited to data required to consider and pursue litigation in support of USERRA and VP enforcement activities.
2. Contractor Access:
 - Contractors have limited access to the production system (Prod) for diagnosing system issues identified by users, but they cannot modify or extract data independently.
 - Contractor Developer(s), Business Analyst(s), and Tester(s) assigned to any contract have full access in Dev, Dev2, Test, and Pre-Production Environments, which do not contain any Personally Identifiable Information (PII).
 3. Role-Based Access:
 - The system employs role-based access, where users are assigned roles based on their required system functions and responsibilities.
 - Additional access is controlled through geographic assignment, limiting visibility to cases within the user's geographic area of responsibility.
 - Privileged User Accounts are assigned to National Office staff responsible for system operation, maintenance, and reports.
 - Managers have access to the files of their employees.
 4. Access Control and Account Management:
 - Access Control/Account Management procedures are in place to manage and monitor access to the system.
 5. Verification of Assignments and Training:
 - Assignments of roles and Rules of Behavior are verified according to established security and auditing procedures.
 - Users must complete the OASAM Rules of Behavior and submit a system access request before being granted access.
 - Requests for account access, modification, and deletion require supervisory and National Office approval.
 - Employees participate in mandatory Privacy Act and Records Management training annually, recorded and tracked in the Department's Learning Link System.
 - Quarterly account certification is conducted to ensure access is routinely reviewed.
 6. Privacy Training:
 - Employees participate in mandatory Privacy Act and Records Management training annually, recorded and tracked in the Department's Learning Link System.
 7. Malicious Auditing Measures and Technical Safeguards:
 - Auditing measures and technical safeguards are in place to prevent misuse of data.
 - Quarterly and annual reviews of finalized data are conducted by the Senior Compliance Analyst and the VCDC.
 - Access Control/Account Management procedures and quarterly account certification help prevent data misuse.
 8. FISMA Compliance:
 - The data is secured in accordance with FISMA requirements.
 - The Security Assessment and Authorization was last reviewed and edited in January 2023.

TECHNOLOGY

The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware, biometrics, and other technology.

- Was the system built from the ground up or purchased and installed?

The VCMS was custom-designed and built from the ground up.

- Describe how data integrity, privacy and security were analyzed as part of the decisions made for your system.

The requirement to implement security and privacy controls were addressed in the system acquisition contract for the VCMS.

- What design choices were made to enhance privacy?

The VCMS employs technical controls and mechanisms, such as encryption, to enhance privacy. The development of roles was done explicitly to limit access to end users based on the principles of least privilege.

- For systems in development, what stage of development is the system in, and what project development life cycle was used?

The VCMS is currently in the Operations and Maintenance phase of the System Development Lifecycle.

- For systems in development, does the project employ technology which may raise privacy concerns? If so, please discuss their implementation?

Not applicable.

DETERMINATION

As a result of performing the PIA, what choices has the agency made regarding the information technology system and collection of information?

The Agency has determined that the safeguards and controls built into the VCMS as a Moderate system adequately protect the information. The Agency has also determined that the VCMS is collecting the minimum necessary information for the proper performance of a documented agency function. Annual reviews of systems controls, and quarterly review of user access will ensure compliance through future Development and Operations and Maintenance stages.

PIA SIGNATURE PAGE

Responsible Officials

Edward Meyman

System Owner VCMS, OASAM

Signature of System Owner

1/10/24

Date

APPENDIX A: DEFINITIONS FOR PII AND PII ELEMENTS THIS SYSTEM COLLECTS

Non-Sensitive PII. PII whose disclosure cannot reasonably be expected to result in personal harm. Examples include first/last name; e-mail address; business address; business telephone; and general education credentials that are not linked to or associated with any protected PII.

Protected PII. PII whose disclosure could result in harm to the individual whose name or identity is linked to that information. Examples include, but are not limited to, social security number; credit card number; bank account number; residential address; residential or personal telephone; biometric identifier (image, fingerprint, iris, etc.); date of birth; place of birth; mother's maiden name; criminal records; medical records; and financial records. The conjunction of one data element with one or more additional elements, increases the level of sensitivity and/or propensity to cause harm in the event of compromise.

What information about individuals will be collected, generated, shared, and/or retained?
Also, note whether the collection is for ☐ Federal employees, ☐ Contractor staff, ☒ Members of the Public {Check all that apply}

- ☒ Prefix or title, such as Mr., Mrs., Ms., Jr. Sr. ☐
- ☒ First name ☒ Middle initial and/or ☒ Last name
- ☒ Name suffix such as Jr. Sr., etc.
- ☒ Date of birth
- ☐ Place of birth
- ☐ Mother's maiden name
- ☒ SSN
- ☒ SSN [truncated]
- ☒ SSN [elongated]
- ☒ Language spoken
- ☒ Military, immigration, or other government-issued identifier
- ☐ Photographic identifiers (i.e., photograph image, x-rays, video)
- ☐ Biometric identifier (i.e., fingerprint, voiceprint, iris)
- ☐ Other physical identifying information (e.g., tattoo, birthmark)
- ☐ Vehicle identifier (e.g., license plate, VIN)
- ☐ Driver's license number
- ☒ Residential address
- ☒ Personal phone numbers (e.g., phone, fax, cell)
- ☒ Mailing address (e.g., P.O. Box)
- ☒ Personal e-mail address

- ☒ Business address
- ☒ Business phone number (e.g., phone, fax, cell)
- ☒ Business e-mail address
- ☒ Medical information including physician's notes
- ☒ Medical record number
- ☐ Device identifiers (e.g., pacemaker, hearing aid)
- ☒ Employer Identification Number (EIN)/Taxpayer Identification Number (TIN)
- ☒ Financial account information and/or number (e.g., checking account number, PIN, retirement, investment account)
- ☒ Certificates (e.g., birth, death, marriage)
- ☒ Legal documents or notes (e.g., divorce decree, criminal records)
- ☒ Educational records
- ☐ Network logon credentials (e.g., username and password, public key certificate)
- ☒ Digital signing or encryption certificate
- ☐ Other: _____
- ☐ None

- Is any part of the PII collection voluntary?

VCMS PII collection is voluntary.

- If any part of the PII collection is voluntary, what efforts are being made to redact, mask, anonymize or eliminate PII from this system?

As the information is used to directly reach points of contact and access is limited to employees responsible for contacting those individuals, no anonymization or masking is feasible.

APPENDIX B: PRIVACY ACT STATEMENT IN VETS 1010 COMPLAIN FORM

OMB NO. 1293-0002 (EXP. 04/30/2026)
VETS USERRA/VP/VEOA Form 1010 (REV 04/2023)

Section K. Punishment for Unlawful Statements

The information provided in this complaint will be utilized by the U.S. Department of Labor, Veterans' Employment and Training Service (VETS) to initiate an investigation of alleged violations of the Uniformed Services Employment and Reemployment Rights Act (USERRA), Title 38, USC, §§ 4301-4335; and/or the laws and regulations relating to veterans' preference in Federal employment, including 5 USC § 3330a-3330c, and eligibility for Federal employment described in the VEOA. Potential claimants should keep in mind that it is unlawful to "knowingly and willfully" make any "materially false, fictitious, or fraudulent statements or representation" to a federal agency. Violations can be punished under Section 2 of the False Statements Accountability Act of 1996 by a fine and/or imprisonment of not more than 5 years. 18 USC § 1001.

Section L. Paperwork Reduction Act Statement

The OMB control number for this collection is 1293-0002 and expires on April 30, 2023. According to the Paperwork Reduction Act of 1995, no person is required to respond to a collection of information unless such collection displays a valid OMB control number.

Collection of this information is authorized by 38 USC § 4326(a) and 5 USC § 3330a(b)(2). The obligation to respond to this collection is required to initiate a USERRA or VP/VEOA investigation. We estimate it takes about 45 minutes to complete this collection of information, including time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information.

Information requested in Section H of this form is voluntary, and not required to initiate an investigation. Information in this section is in response to Executive Order 13985 - Advancing Racial Equity, and Support for Underserved Communities Through the Federal Government. Information collected within this section will be used to provide better training to investigators to better serve underserved populations.

Please send comments regarding the burden estimate or any other aspect of this collection of information to the Veterans' Employment and Training Service, 200 Constitution Ave NW, Room S-1325, Washington, DC 20210 or VETSCompliance@dol.gov and reference OMB control number 1293-0002.

Note: If this form can only be submitted by mail, please see instructions for submission by mail in the VETS USERRA/VP Form 1010(a).

Section M. Privacy Act Statement

The primary use of this information is by staff of the Veterans' Employment and Training Service in investigating cases under USERRA, or the laws and regulations relating to VP or VEOA in Federal employment. Disclosure of this information may be made to: a Federal, state or local agency for appropriate reasons; in connection with litigation; and to an individual or contractor performing a Federal function. Furnishing the information on this form, including your Social Security Number, is voluntary. However, failure to provide this information may jeopardize the Department of Labor's ability to provide assistance or complete an investigation of your complaint.

Section N. Notification of Claimant's Rights

For claims arising under USERRA, a person has a right to commence an action for relief directly against the employer in the appropriate federal district court (in the case of a complaint against a State or private employer), pursuant to 38 USC § 4323(a)(3), or the Merit Systems Protection Board (in the case of a complaint against a Federal executive agency or the Office of Personnel Management), pursuant to 38 USC § 4324(b).

For claims arising under VP or VEOA, a person may file a complaint with the Secretary of Labor within 60 days after the date of the alleged violation, pursuant to 5 USC § 3330a(a). The Secretary shall investigate the complaint under 5 USC § 3330a(b), and, if unable to resolve the complaint within 60 days, the Secretary will notify the person of the results of the investigation, pursuant to 5 USC § 3330a(c). The person may appeal to the Merit Systems Protection Board on or after the 61st day after the complaint was filed with the Secretary, but not later than 15 days after the person receives notification from the Secretary of the results of the investigation, pursuant to 5 USC § 3330a(d).

Section O. Certification and Signature

By my signature I certify that the above information is true and correct to the best of my knowledge and belief. I authorize the U.S. Department of Labor to contact the employer identified in Section B or any other person with information concerning this claim. I further authorize my employer or any other person to release such information to the U.S. Department of Labor. Pursuant to 5 USC, § 552a(b) of the Privacy Act, I authorize the U.S. Department of Labor, the U.S. Department of Veterans Affairs, and the U.S. Department of Defense to release information and records necessary for the investigation and prosecution of my claim.

1. Signature

2. Date

Clear Form

Submit Form

Save Form