PRIVACY IMPACT ASSESSMENT

Effective Date: March 3, 2026

Veterans' Employment and Training Service (VETS)
VETS Grantee Reporting System (VGRS)

✔ Concurrence of Senior Agency Official for Privacy

☐ Non-concurrence of Senior Agency Official for Privacy

BRAYE CLOUD

Digitally signed by BRAYE CLOUD
Date: 2026.03.03 11:55:33 -05'00'

Braye Cloud, Senior Agency Official for Privacy (SAOP)
Deputy Assistant Secretary for Operations
Office of the Assistant Secretary for Administration & Management

OVERVIEW & GENERAL INFORMATION

As required by the E-Government Act of 2002 (as amended) and OMB Memorandum M-03-22, VETS has developed this Privacy Impact Assessment to describe:

1. The information to be collected with a particular focus on personally identifiable information (PII);
2. Why the information is being collected including the legal authority for the information collection;
3. The intended use of the information;
4. With whom the information will be shared (such as internal uses with other DOL component agencies or another federal agency);
5. What notice is provided to individuals, what opportunities are given to individuals to consent to particular uses of the information, how individuals can grant consent, and what opportunities individuals have to decline to provide information;
6. How the information will be secured with administrative and technological security controls;
7. Whether a *system of records* is being created under the Privacy Act, 5 U.S.C. 552a; and
8. The analysis of privacy risk associated with the collection, use, storage, and dissemination of information and practices that have an impact on privacy.

Name of System (and Acronym, if applicable)

VETS Grantee Reporting System (VGRS CSAM ID # 2735)

Location of the System

The VETS Grantee Reporting System (VGRS) is hosted on a DOL Platform. Appian Corporation manages the DOL Platform environment on their Government Cloud solution. The system is accessible anywhere where a DOL-issued Government Furnished Equipment (GFE) is operable.

Brief Description of the System

VETS Grantee Reporting System (VGRS) is a new DOL information technology system that supports the management of quarterly performance reporting for the VETS Homeless Veterans' Reintegration Program (HVRP). The system has replaced the VETS-701 Technical Performance Report (TPR) and VETS-702 Technical Performance Narrative (TPN). These were Excel and PDF based information collection forms that required an email-based grant reports submission process to perform the program's quarterly reporting. VGRS has eliminated this process and provides grant recipients and VETS users with one location in which mandatory data is collected all while providing a consistent end user experience and allow for the creation and submission of reports through a process flow.

The system serves approximately 950 users. These users are broken down into two categories: external and internal users. External users are all grant recipient staff accessing the system through login authentication; these users use the application to input grant-related data to create

performance reports for submission to VETS state and regional users. Internal users are VETS staff and contractors who use the system's workflow feature to review, approve/certify submitted reports, and extract data for analysis.

Purpose of the System:

☒ Program administration	☐ Employee or customer satisfaction surveys
☐ Computer Matching Program	
☐ Administering human resources programs for DOL or federal government personnel	☐ Improve Federal services online
☐ Litigation	☐ Promote information sharing initiatives
☐ Criminal law enforcement activities	☐ Civil law enforcement activities
☐ Other: Specify	

This System is operated by:

☒ Component agency: Veterans' Employment and Training Service (VETS)

☐ Contractor

For a system operated by a contractor, the contract or other acquisition-related documents includes privacy requirements:

☐ Yes
☐ No

This PIA is being conducted for:

☐ A new information system or project that collects, maintains, or disseminates information in identifiable form.

☐ A new collection of information subject to the Paperwork Reduction Act because it is for 10 or more persons (excluding agencies, instrumentalities, or employees of the federal government in the scope of their employment).

☐ A change to the PII Confidentiality Impact Level (NIST SP 800-122) or System Security Categorization (NIST SP 800-60).

☐ An existing system subject to a periodic review at the 5-year mark.

☒ An existing system with significant changes that create new privacy risks.

The following are the significant changes that create new privacy risks:

☐ Changed information collection authorities.

☐ Changed business processes.

☒ Conversion of paper-based records to electronic systems.

☐ Anonymous to Non-Anonymous. This is when functions applied to an existing system change anonymous information into information in identifiable form.

☐ Significant System Management Changes. This is when new uses of an existing IT system, including application of new technologies, significantly change how information in identifiable form is managed in the system.

☐ Significant Merging. This is when agencies adopt or alter business processes so that government databases holding information in identifiable form are merged, centralized, matched with other databases or otherwise significantly manipulated.

☐ New Public Access. This is when user-authenticating technology (e.g., password, digital certificate, biometric) is newly applied to an electronic information system accessed by members of the public.

☐ Commercial Sources. This is when agencies systematically incorporate into existing information systems databases of information in identifiable form purchased or obtained from commercial or public sources.

☐ New Interagency Uses. This is when agencies work together on shared functions involving significant new uses or exchanges of information in identifiable form.

☐ Internal Flow or Collection. This is when alteration of a business process results in significant new uses or disclosures of information or incorporation into the system of additional items of information in identifiable form.

☐ Alteration in Character of Data. This is when new information in identifiable form added to a collection raises the risks to personal privacy (for example, the addition of health or financial information).

☐ Other:

The class(es) of users who will have access to the system are:

General Public
☒ Contractors
☒ Government Employees
☐ Other:

1. INFORMATION IN THE SYSTEM

VGRS collects grant related information pertaining to the Grantee Organization, Grantee Organization Staff, and individual participants.

1.1. The information that is collected, used, maintained, or disseminated by in connection with the system is:

☒ Name/Former Name	☒ Date of Birth	☐ Maiden Name	☐ Place of Birth	☐ Citizenship
☐ Social Security number (including in truncated form)	☐ Driver's License	☐ Financial Account	☐ Taxpayer ID	☐ Passport Number
☒ Sex	☐ Telephone Number	☐ Criminal Record	☐ Education	☒ Age
☐ Financial Transaction	☒ Employer ID	☐ Alien Registration Number	☐ Vehicle Identifier	☐ Employee ID
☐ Credit Card	☐ Medical Record	☐ File/Case ID	☐ Financial Information	☐ Religion
☐ Alias	☐ Home Address	☒ Military Service	☐ Mother's Maiden Name	☒ Medical Information
☐ Email Address	☐ Marital Status	☒ Race/Ethnicity	☒ Occupation	☒ Work Email Address
☒ Job Title	☒ Salary	☐ Business Associates	☒ Work Telephone Number	☐ Proprietary or Business Information
☐ Employment Performance Ratings	☒ Work Address	☒ Work History	☐ Procurement or contracting records	☐ Other Performance Information
☐ Fingerprints	☐ Scars, Marks, Tattoos	☐ Signatures	☐ Photographs	☐ Palm Prints
☐ Hair Color	☐ Vascular Scans	☐ Weight	☐ Voice/Audio Recording	☐ Eye Color
☐ DNA Sample or Profile	☐ Dental Profile	☐ Video Recording	☐ Height	☐ Retina/Iris Scans
☒ User ID	☐ IP Address	☒ Other PII: First and Middle initial, first four characters of last name		

1.2. The information is collected using the following methods:

☒ Website-based forms: DOL does not collect the information directly from the participant (individual that the performance data is about). Grantee Organization Staff will collect the information from the participants (individuals) via web forms.
☐ Paper forms
☐ Electronic forms
☐ Verbal collection
☐ No form - the information collected does not require a specific form

1.3. The source of the information is:

Directly from the Individual about Whom the Information Pertains		
☐ In Person	☐ Hard Copy: Mail/Fax	☐ Web-based (uploading through an app or website)
☐ Telephone	☐ Email	☐ Legal or other representative:
☐ Other:		

Government Sources		
☐ Within the Component Agency	☐ Other DOL component agencies	☐ Other Federal Agencies
☐ State, Local, Tribal	☐ Foreign	☐ Other:

Non-government Sources		
☒ Public Organizations	☐ Private Sector	☐ Commercial Data Brokers
☐ Third Party Website or Application	☒ Other: Public Organizations collect information from the participants in various ways. Various ways can include but are not limited to in person, email, phone calls etc.	

1.4. Social Security numbers (SSN) are collected:

The Privacy Act of 1974 requires that when DOL requests that an individual provide a Social Security number, DOL must indicate whether that disclosure is mandatory or voluntary and by what statutory or other authority the number is being requested including what uses will be made of it.

Additionally, OMB Circular A-130 to the Heads of Executive Departments and Agencies regarding *Managing Information as a Strategic Resource* includes a requirement that DOL take steps to eliminate unnecessary collection, maintenance, and use of Social Security numbers, and explore alternatives to the use of Social Security numbers as a personal identifier.

Finally, DOL policies permit component agency programs to collect, use, maintain, and disseminate SSNs only when required by law (e.g., statute, regulation, or upon approval of the SAOP or SAOP designee).

Will SSNs be collected for this system, whether directly or indirectly from the individual to whom the SSN applies?

☒ No

☐ Yes

1.4.1. If yes, the specific authority relied upon to collect SSNs?

N/A

1.4.2. The purpose for the collection of SSNs and how the SSN will be used is as follows:

N/A

1.4.3. The following alternatives were considered in lieu of the collection of SSNs:

N/A

1.4.4. The alternatives were not selected because:

N/A

1.5. The information collected is subject to the Paperwork Reduction Act:

☒ Yes, some or all of the information is covered by the Paperwork Reduction Act.

- ☐ The information expected to be collected does not yet have an OMB control number but will be submitted for PRA approval.
- ☒ The information collected is part of an existing collection and the OMB control number for the collection is: 1293-0014 VETS Competitive Grant Program Reporting

☐ No, the information collected is not subject to the Paperwork Reduction Act.

2. WHY THE INFORMATION IS BEING COLLECTED

2.1. Why is the information being collected?

The collection of information is necessary for the proper oversight of discretionary grant funds administered by the DOL VETS as required by law and regulation. These discretionary grants fund over

160 HVRP projects that serve nearly 17,000 veterans experiencing homelessness, veterans at-risk of homelessness, and incarcerated veterans annually.

HVRP is authorized under 38 USC 2021. The collection of program data is mandated under 38 USC 2021(b). The Homeless Women Veterans and Homeless Veterans with Children Reintegration grant program (HWVHVWC) is authorized under 38 USC 2021A. The collection of program data is mandated under 38 USC 2021A(c).

There are two administrative provisions in Title 29 of the Code of Federal Regulations (CFR) related to the monitoring and reporting of program performance: in reports, records retention and enforcement: 29 CFR 97.40 and in post-award requirements – reports and records: 29 CFR 95.51. Additionally, Title 2 of the CFR authorizes data collection for performance measurement related to goals, indicators, targets, and baseline data in 2 CFR 200.301.

2.2. The following are the specific legal authorities and/or agreements that permit the collection, use, maintenance, and/or dissemination of information (including any PII) by the system:

Homeless Veterans Reintegration Programs, 38 USC §2021 and 38 USC §2021A
2 CFR §200.301 and 29 CFR 95.51

3. INTENDED USE OF THE INFORMATION

3.1. The information collected by the system is used in the following ways:

The information is used for reporting program services and outcomes to Congress. 38 USC 2021(g) and (h) requires an annual report to Congress that contains a report on the number of HVRP participants served by sex, age, race, ethnicity, approximate era in which the veteran served in the Armed Forces, the highest level of education attained, the average period of time the veteran was unemployed or underemployed before receiving services under this section and while receiving such services, housing status as of the date on which the veteran is first enrolled and any subsequent date; all disaggregated by geographic location.

3.2. The system aggregates or analyzes information to create new information:

☐ Yes:
☒ No

4. INFORMATION SHARING AND ACCESS

4.1. Will VETS share data with internally or externally?

☐ Yes, the PII in the system will be shared.
☒ No, The PII in the system will not be shared.

Internal Sharing:

Component Agency	Information Shared	Purpose

External Sharing:

Organization	Information Shared	Purpose	MOU or other Agreement

4.2. Does the VETS place a limitation on re-dissemination of PII shared with internal or external organizations?

Internal Sharing

☐ Yes, another DOL component agency is required to verify with the component agency operating the system before re-dissemination of PII.

☐ No, another DOL component agency is not required to verify with the component agency operating the system before re-dissemination of PII.

☒ Not applicable, the component agency does not share PII with other DOL component agencies.

External Sharing

☐ Yes, the external agency or entity is required to verify with the DOL component agency before re-dissemination of PII.

☐ No, the external agency or entity is not required to verify with the DOL component agency before re-dissemination of PII.

☒ Not applicable, the component agency does not share PII with external agencies or entities.

4.3. Indicate whether the system connects with or receives information from any other systems authorized to process PII.

☐ Yes, this system connects with or receives information from another system(s) authorized to process PII.

If the answer to 4.3 is yes, provide the name of the system and describe the technical controls which prevent improper accessing of the PII while in transit.

☒ No, this system does not connect with or receive information from another system(s) authorized to process PII and/or BII.

5. NOTICE, CONSENT, AND OPPORTUNITY TO DECLINE TO PROVIDE INFORMATION

5.1. Indicate whether individuals will be notified if their PII is collected, maintained, or disseminated by the system.

☐ Notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 7.

☐ Notice is provided by a Privacy Act Statement and/or a Privacy Notice. The Privacy Act Statement and/or Privacy Notice can be found on the following forms or information collection instruments:

☒ Notice is provided by other means.

The individual participant whose information is collected may be provided notice outside of VGRS by the grant recipient. Veterans' Program Letter *06-24 HVRP Requirements & Functions* states that "Grant recipients must protect participants' privacy to the greatest extent possible following the steps outlined in their grant award's terms and conditions and the legal requirements contained in the Funding Opportunity Announcement (FOA) under which the award was issued." The *Terms and*

Conditions of their award require adherence to *TEGL 39-11 Guidance on Handling and Protection of PII*.

☐ Notice is provided by means of this Privacy Impact Assessment.

5.2. Do individuals have an opportunity to decline to provide PII?

☐ Yes, individuals have an opportunity to decline to provide PII.

☒ No, the individual does not have the opportunity to decline to provide PII because PII is required for the grant recipient to determine the individual's eligibility for enrollment (receiving of services and/or training funded by the grant).

5.3. Do individuals have an opportunity to consent to particular uses of their PII?

☐ Yes, individuals have an opportunity to consent to particular uses of their PII.

☒ No, the individual does not have the opportunity to consent to particular uses of their PII because PII is required for the grant recipient to determine the individual's eligibility for enrollment (receiving of services and/or training funded by the grant).

5.4. Do individuals have an opportunity to review or update PII pertaining to them?

☒ Yes, individuals have an opportunity to review or update PII pertaining to them.
The individual may notify the grant recipient to update PII elements related to their enrollment and Grantee Organization Staff may edit applicable entries within the system.

☐ No, individuals do not have an opportunity to review or update PII pertaining to them.

6. HOW INFORMATION IS SECURED

As required by the E-Government Act of 2002 and OMB Memorandum M-03-22, DOL imposes certain administrative and technological controls on each system that contains PII. Below, DOL describes whether it has conducted a risk assessment, the security controls to put in place to protect against that risk, and how those controls are implemented. DOL also describes how it continuously monitors the system to ensure that the controls continue to work properly, safeguarding the information. Individuals who have questions regarding the information below may reach out to DOL's Privacy Program at privacy@dol.gov.

6.1. Administrative controls for the system:

☒ PII is kept in a secured physical location.

The PII is stored in a DOL Cloud Environment.

☒ All users signed a confidentiality agreement or non-disclosure agreement.
All DOL Employees and Contractors must sign confidentiality and non-disclosure agreements upon employment with DOL. Non-DOL users are not prompted by DOL to sign a confidentiality agreement or non-disclosure agreement. However, non-DOL users may be required to sign a confidentiality agreement or non-disclosure agreement through their employers.

☒ All users are subject to a Code of Conduct that includes the requirement for confidentiality.
All DOL Employees and Contractors must sign confidentiality and non-disclosure agreements upon employment with DOL; also, when requesting system access, must approve a Code of Conduct that notes the proper usage of the system. All users must agree to DOL's Rules of Behavior prior to using the system which notates the proper usage of the system.

☒ DOL Personnel (employees, contractors, interns, volunteers) receive **annual** training on privacy and confidentiality policies and practices.
All DOL employees/contractors are required to take the annual DOL Cybersecurity and Privacy Awareness Training (CSPA).

☐ DOL Personnel receive **role-based** training on privacy and confidentiality policies and practices.

☒ DOL Personnel (employees, contractors, interns, volunteers) receive **system-specific** training on privacy and confidentiality policies and practices.
There are system specific training courses available for DOL personnel on an internal VETS SharePoint and for grant recipients on the DOL VGRS webpage including user guides and training videos.

☒ Access to the PII is restricted to authorized personnel only.
DOL users (Federal Staff and Contractors) have access most PII in the system except for a participant's date of birth. Grantee Staff users only have access to the PII in the Grant Record they have been provided access to (a user must be assigned to the Grantee Organization and have been provided access to the Grant Record) which Grantee Staff users have input into the system.

☐ Appropriate NIST SP 800-53 Revision 4 security controls for protecting PII are imposed.
- ☐ A security assessment report has been prepared for the information system to identify all privacy risks for continuous monitoring.

☒ Appropriate NIST SP 800-53 Revision 5 security controls for protecting PII are imposed.
The controls are imposed during the ATO process.
- ☒ A security assessment report has been prepared for the information system to identify all privacy risks for continuous monitoring.
  VGRS has completed the FY24 Security Assessment and received a SAR.

☒ There is one or more Plan of Action and Milestones (POA&M) associated with this system.
POA&Ms have been created to address findings from the FY24 Security Assessment and will continue to be created following future security assessments or vulnerability scans. The completion of this PIA will resolve most of the existing POA&Ms for VGRS.

☒ Contractors that have access to the system are subject to information security provisions in their contracts required by DOL policy.
1605C4-25-F-00004 VETS Analysis, Performance, Policy, & Administrative Support (VAPPAS) contract includes section 1.6.10.4 Privacy Act Notification, 1.6.10.6 Cybersecurity and Privacy Training, and

1.6.11 Privacy Act Notification re: PII data located within IT systems, software, research data/information, documentation, personnel, and facilities.

1605C5-21-F-00033 National Veterans' Technical Assistance Center (NVTAC) contract includes a clause for Contractor Personnel Telework (January 2020) that requires all contract staff to employ appropriate safeguards and comply with all applicable DOL and Federal policies, requirements, and procedures related to Personally Identifiable Information, security, network, data, and communications.

☐ Contracts with customers establish DOL ownership rights over data including PII.

☐ Other:

6.2. Technological controls for the system:

☒ Access to the PII is being monitored, tracked, or recorded:
All user activity within the system is captured in the audit logs.

☒ User Log In Credentials
DOL users (both federal and contractors) access the DOL network using their credentials. Further authentication into DOLs Platform is managed using Active Directory Authentication to perform login authentication).

☒ Virtual Private Network (VPN)
Internal users must authenticate using the DOL network.

☐ Biometrics

☒ Encryption of Data at Rest
Data is encrypted at rest.

☐ Firewall

☒ Role-based Access Controls
VGRS lists out the roles and what each role can do in the SSP and Account Management SOP.

☒ Encryption of Data in Transit
All data in transit is encrypted.

☒ Use Only for Privileged (Elevated Roles)
VGRS lists out the roles and what each role can do in the SSP and Account Management SOP.

☐ Other:

6.3. Retention of Information

Information in the system is covered by an approved records retention schedule and monitored for compliance.

☒ Yes.
General Records Schedule GRS 1.2 item 010 Grant and cooperative agreement program management records (DAA-GRS-2013-0008-0007) states the disposition instruction is to be

destroyed 3 years after final action is taken on the file, but longer retention is authorized if required for business use.

☐ No.

☐ A records retention schedule is in development.

If there is an approved record retention schedule, is retention monitored for compliance to the schedule?

☒ Yes, retention is monitored for compliance to the schedule.

☐ No, retention is not monitored for compliance to the schedule.

☐ No, there is not an approved record retention schedule.

When information is no longer needed, it is disposed of by:

☐ Shredding or other physical destruction

☐ Overwriting

☐ Physical destruction of hardware, such as degaussing

☒ Deleting

☐ Other:

7. SYSTEM OF RECORDS NOTICE (SORN)

The Privacy Act of 1974 (Privacy Act) requires DOL to permit individuals to gain access to their records (including obtaining copies and requesting amendments to the records) and any information pertaining to the requesting individual which is contained in a "system of records" (a specifically defined term under the Privacy Act). Although many DOL Information Systems may contain PII, they are not all required to have a SORN. For purposes of the Privacy Act, a system of records that requires a SORN refers to any group of any records under the control of DOL (including through a contractor) from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual. Some systems of records under DOL's control may be exempt from some of the Privacy Act rights provided to individuals. DOL is identifying all of the SORNs applicable to this system so that individuals may review the SORNs for more detailed additional information.

7.1. This system is covered by one or more existing SORNs.

A SORN is in development.

7.2. This system:

☐ Does not require an additional SORN beyond those identified above.

☐ Does not require a SORN.

☐ Requires an additional new SORN.

☐ Requires a modification to the following SORN(s):

Reason for Modifying SORN(s):

☐ A significant increase in the number, type, or category of individuals about whom records are maintained.
☐ A change that expands the types or categories of information maintained.
☐ A change that expands the types or categories of information maintained.
☐ A change that modifies the scope of the system.
☐ A change that modifies the purpose(s) for which the information in the System of Records is maintained.
☐ A change in the agency's authority to maintain the system, collect, use, or disseminate the records in the system.
☐ A change that modifies the way in which the system operates or its location(s) in such a manner as to modify the process by which individuals can exercise their rights under the statute.
☐ A change to equipment configuration (either hardware or software), storage protocol, type of media, or agency procedures that expands the availability of, and thereby creates substantially greater access to, the information in the system.
☐ The addition or rescindment of a Privacy Act exemption.
☐ A new routine use or significant change to an existing routine uses that has the effect of expanding the availability of the information in the system.

8. ANALYSIS OF PRIVACY RISK

8.1. PII Confidentiality Impact Level from NIST Special Publication 800-122

Indicate the potential impact that could result to the subject individuals and/or DOL if PII were inappropriately accessed, used, or disclosed.

☐ **Low** – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
☒ **Moderate** – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
☐ **High** – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

8.2. Identification and evaluation of potential risks to privacy

Adequacy of Privacy Training for DOL personnel

All DOL personnel, including VGRS users, are required to take annual Cybersecurity and Privacy Awareness Training. VGRS users with elevated security or privacy roles/responsibilities are required to take role-based training. There are system specific training courses available for DOL personnel on an internal VETS SharePoint and for grant recipients on the DOL VGRS webpage including user guides and training videos.

How Information is Acquired, Stored, and Shared

The information is acquired from Grantee Organization Staff; they collect the information from individuals and input it into the VGRS system. Information is stored securely in the DOL Cloud Environment, following NIST 800-53 Rev 5 requirements. The information is not shared internally or externally.

Describe the choices that were made with regard to preventing or mitigating these privacy risks

VETS attended to all potential privacy risks while completing this PIA. VETS uses the minimum required PII to serve its purpose and adheres to the NIST 800-53 Rev 5 security and privacy control requirements. All user activity within the system is captured in the audit logs. User roles are assigned within the system to limit access to PII on a need-to-know basis. DOL users (both federal and contractors) access the DOL network using their credentials. External users authenticate onto the system via login authentication. All data in the system is encrypted. All DOL Employees and Contractors must sign confidential and non-disclosure agreements upon employment with DOL. All DOL employees and contractors take annual Cybersecurity and Privacy Awareness training. In addition to this, DOL offers role-based training to elevated roles, and system specific trainings are available as well.

Protection against PII Breaches

Unauthorized Data Access:

The system has established role-based access controls and privileged access roles. This allows only specifically approved users to have access to the system and view PII. The data that is in transit and at rest is encrypted to prevent unauthorized access. All user activity within the system is captured in the audit logs. DOL users (both federal and contractors) access the DOL network using their credentials. External users authenticate onto the system via login authentication.

Potential Misuse of Data:

All users of VGRS must accept rules of behavior prior to gaining access to the system. System activities are monitored in the audit logging process. VGRS assigns privileged access roles and user roles to limit access to the system. The data is encrypted when it is in transit and at rest.

Protecting Against Insider Threats:

Federal staff can view all records within VGRS but are limited to what they are able to manage (create/edit/delete). This includes some limitations in what they are able to view; for example, some roles are blocked from viewing a participant's date of birth.

In addition to this, users with elevated privileges are audited. There are a few users with this level of access, and it is confined to VGRS, meaning other DOL users with a similar level of access in other DOL systems are unable to access VGRS just as the VGRS users with elevated privileges are unable to access the other DOL systems.

There is no database access in the production environment.

Describe the choices that were made with regard to preventing or mitigating these privacy risks

VETS collects and uses the minimum amount of PII required to execute the agency's grant programs' reporting requirements. Participants do not directly input their PII but provide it to grant recipients who input the information into VGRS as part of their grant reporting requirements. In addition, the system provides role-based access controls.

Other: N/A

Describe the choices that were made with regard to preventing or mitigating these privacy risks

N/A

SIGNATURE PAGE

Reviewed by: Rhonda Epps, Executive Director, VETS Office of Field Operations

Rhonda L. Epps Digitally signed by Rhonda L. Epps Date: 2026.02.24 12:01:00 -05'00'

Signature

Reviewed by: Tim Erskine, Director of Mission Support, OASAM-OCIO

TIMOTHY ERSKINE Digitally signed by TIMOTHY ERSKINE Date: 2026.02.25 13:57:05 -05'00'

Signature

Reviewed by: Mara Blumenthal, DOL Privacy Office OASAM-OCIO

MARA BLUMENTHAL Digitally signed by MARA BLUMENTHAL Date: 2026.02.25 12:43:14 -05'00'

Signature