Privacy Impact Assessment for the VA IT System called:

Digital GI Bill (DGI)
VBA Education Service (EDU)/
Software Product Management (SPM)
eMASS ID # 1454

Date PIA submitted for review:

March 08, 2024

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	*Marvis Harvey*	*marvis.harvey@va.gov*	*202-461-8401*
Information System Security Officer (ISSO)	*Bobbi Begay*	*Bobbi.Begay@va.gov*	*720-788-4518*
Information System Owner	*Riley Ross*	*Riley.Ross@va.gov*	*918-869-5448*

Abstract

The Digital GI Platform (DGI) Managed Services information system has a system categorization of Moderate. It enables the VA to improve timely and accurate delivery of educational payments and determine real-time eligibility and benefit information. The platform will also provide the ability for GI Bill students to engage with VA through electronic outreach, intake and upgraded communication tools for on-the-spot service. As well as provide the VA with an end-to-end systems management perspective to ensure proper compliance and oversight of GI Bill programs, and the use of data and business intelligence tools to track, monitor and measure school and student outcomes. The system runs on top of AWS GovCloud and is tightly integrated with other SaaS services such as Mulesoft, Dynatrace and Accenture XDR.

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?

Digital GI Bill (DGI) is a managed service system under VBA Education Service (EDU) and Software Product Management (SPM).

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

The system houses the applications which are used to process the benefits of the Post-9/11 Veterans Educational Assistance Act of 2008. The DGI system provides an integrated solution of Education Benefit Information records between the systems of the Veterans Benefits Administration (VBA) using a single point of entry.

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

The Digital GI Bill Platform (DGI) is a managed service environment owned and operated by Accenture Federal Services for the exclusive use of the Department of Veteran Affairs (VA). The solution is authorized for use by the VA under VBA Education Service (EDU) and Software Product Management (SPM).

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?

The DGI currently houses the educational benefits information for 3.5 – 4 million veterans. Users of the DGI are VA Claim Evaluators (VCEs) at Regional Processing Offices (RPOs); School Certifying Officials (SCOs) at educational institutions across the United States

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

The information in the DGI includes individual identifiers and contact information to be used for benefit determination and communications with Veterans.

F. What information sharing conducted by the IT system? A general description of the modules and subsystems, where relevant, and their functions.

The DGI connects with the following information systems to fulfill the promise of educational benefits for Veterans in an efficient time frame:

- Identity and Access Management (IAM)
- VA DoD Identity Repository (VDR)
- Benefits Delivery Network (BDN)
- Common Security Services (CSS)
- VBA Corporate Infrastructure (CRP/BEP)
- AITC Facility (AITC)
- VA Performance Analysis and Integrity Reporting (PA&I) Business Intelligence (VD3)
- Veterans-Facing Services Platform-Va.gov (VFSP-Va.gov)
- VA Profile
- BIP Assessing (BIP) – eMPWR-VA
- CSOC Vulnerability Scanning System Assessing (CSOC VSS)

Additionally, the DGI is comprised of cloud-based components noted below:

- AWS GovCloud – Infrastructure Services for DGI
- Mulesoft – API Integration
- DynaTrace – Application Performance Monitoring and Tracing
- Duo Federal – Multi Factor Authentication Provider
- Accenture XDR – Security Monitoring Services
- SentinelOne – Application Protection
- Twilio – SMS Messaging Provider

G. 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 DGI is operated in a highly available architecture spanning across three Amazon Web Services (AWS) Availability Zones (AZs) within the US-GOV-WEST-1 region. DGI aims to maximize the user experience, provide a flexible design to support benefit changes, provide an efficient workflow, and support programming integration across future VA projects. DGI minimizes manual intervention and maximizes efficiency of the process while meeting the needs of the VA for the long term. Users of the DGI are VA Claim Evaluators (VCEs) at Regional Processing Offices (RPOs); School Certifying Officials (SCOs) at educational institutions across the United States, as well as DGI administrators and development teams who monitor and maintain the infrastructure, software and processes that comprise the DGI. Future use cases will also provide for direct Veteran and Beneficiary access.

The VA has contracted with Accenture Federal Services (AFS) to provide a managed service environment to process educational claims on behalf of the VA. AFS contracts with AWS to maintain the underlying hardware required to provide DGI's underlying virtualized environments. DGI administrators can manage the virtual machines and network configurations through a secure Graphical User Interface (GUI) console. The AWS console allows authorized DGI systems, database, and security administrators to access the environment through the Web and manage the systems in AWS GovCloud West. All data contained within the DGI system, PII included, is owned by the VA.

3. Legal Authority and SORN

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

SORN 58VA21/22/28 states authority for the DGI is: Title 10 United States Code (U.S.C.) chapters 106a, 510, 1606 and 1607 and Title 38, U.S.C., section 501(a) and Chapters 11, 13, 15, 18, 23, 30, 31, 32, 33, 34, 35, 36, 39, 51, 53, and 55 (https://www.oprm.va.gov/privacy/systems_of_records.aspx).
2021-24372.pdf (govinfo.gov)

I. 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?

- No, the SORN does not require amendment. The SORN does cover cloud usage.

4. System Changes

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

No

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

No

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:

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

VA_PERSON_ID
VA_FILE_NUMBER
SOCIAL_SECURITY_NUMBER
FIRST_NAME
LAST_NAME
MIDDLE_NAME
DATE_OF_BIRTH
DATE_OF_DEATH
GENDER
ADDRESS_LINE_1
ADDRESS_LINE_2
ADDRESS_LINE_3
CITY
STATE_CODE_KEY
ZIPCODE
PRIMARY_PHONE_NUMBER
SECONDARY_PHONE_NUMBER
HOME_PHONE
MOBILE_PHONE
EMAIL_ADDRESS
BRANCH_OF_SERVICE
BASD_DATE (Basic Active Service Date)
CHARACTER_OF_SERVICE
REASON_FOR_SEPARATION
POWER_OF_ATTORNEY_NAME
TRANSFEROR_DATE_OF_DEATH
USERID
USERNAME/EMAIL
CURRENT_FIRST_NAME
CURRENT_LAST_NAME
PREVIOUS_FIRST_NAME
PREVIOUS_LAST_NAME
DIRECT DEPOSIT ACCOUNT TYPE
DIRECT DEPOSIT ACCOUNT NUMBER
DIRECT DEPOSIT ROUTING NUMBER
DEP_CHILD_DOB
DEP_CHILD_NAME
DEP_CHILD_STAT
DISAB_EXT_DATE
SPOUSE_NAME

PII Mapping of Components (Servers/Database)

Within each environment, the DGI store of PII consists primarily of the Oracle database which resides within the AWS GovCloud environment for DGI as well as additional components and cloud services which make up the DGI managed service ecosystem. Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by DGI 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**
Automation	No	Yes	DIRECT_DEPOSIT_ACCOUNT DIRECT_DEPOSIT_ROUTING	Automated processing of claims	Encrypted Tablespaces Hardware encryption of volumes
BA Reporting (4)	No	Yes	VA_PERSON_ID VA_FILE_NUMBER SOCIAL_SECURITY_NUMBER FIRST_NAME LAST_NAME MIDDLE_NAME DATE_OF_BIRTH DATE_OF_DEATH TRANSFEROR_DATE_OF_DEATH GENDER ADDRESS_LINE_1 ADDRESS_LINE_2 ADDRESS_LINE_3 CITY STATE_CODE_KEY ZIPCODE MOBILE_PHONE HOME_PHONE EMAIL_ADDRESS BRANCH_OF_SERVICE BASD_DATE CHARACTER_OF_SERVICE REASON_FOR_SEPARATION POWER_OF_ATTORNEY_NAME	Consolidated data storage for real time reporting	Encrypted Tablespaces Hardware encryption of volumes
CDS (4)	No	Yes	VA_PERSON_ID VA_FILE_NUMBER SOCIAL_SECURITY_NUMBER FIRST_NAME LAST_NAME MIDDLE_NAME DATE_OF_BIRTH DATE_OF_DEATH	Consolidated data storage for real time reporting	Encrypted Tablespaces Hardware encryption of volumes

			TRANSFEROR_DATE_OF_DEATH GENDER ADDRESS_LINE_1 ADDRESS_LINE_2 ADDRESS_LINE_3 CITY STATE_CODE_KEY ZIPCODE MOBILE_PHONE HOME_PHONE EMAIL_ADDRESS BRANCH_OF_SERVICE BASD_DATE CHARACTER_OF_SERVICE REASON_FOR_SEPARATION POWER_OF_ATTORNEY_NAME		
CH33 (8)	Yes	Yes	VA_PERSON_ID VA_FILE_NUMBER SOCIAL_SECURITY_NUMBER FIRST_NAME LAST_NAME MIDDLE_NAME DATE_OF_BIRTH DATE_OF_DEATH GENDER ADDRESS_LINE_1 ADDRESS_LINE_2 ADDRESS_LINE_3 CITY STATE_CODE_KEY ZIPCODE PRIMARY_PHONE_NUMBER SECONDARY_PHONE_NUMBER EMAIL_ADDRESS BRANCH_OF_SERVICE BASD_DATE (Basic Active Service Date) CHARACTER_OF_SERVICE REASON_FOR_SEPARATION	Required for claimant benefit generation	Encrypted Tablespaces Hardware encryption of volumes
Claimant (6)	No	Yes	VA_PERSON_ID VA_FILE_NUMBER SOCIAL_SECURITY_NUMBER FIRST_NAME LAST_NAME MIDDLE_NAME DATE_OF_BIRTH DATE_OF_DEATH TRANSFEROR_DATE_OF_DEATH GENDER ADDRESS_LINE_1 ADDRESS_LINE_2 ADDRESS_LINE_3 CITY STATE_CODE_KEY ZIPCODE MOBILE_PHONE HOME_PHONE EMAIL_ADDRESS BRANCH_OF_SERVICE	Required for claimant benefit generation	Encrypted Tablespaces Hardware encryption of volumes

			BASD_DATE CHARACTER_OF_SERVICE REASON_FOR_SEPARATION POWER_OF_ATTORNEY_NAME DEP_CHILD_DOB DEP_CHILD_NAME DEP_CHILD_STAT		
Notification (7)	Yes	Yes	EMAIL_ADDRESS FIRST_NAME LAST_NAME MOBILE_PHONE	Required to send email and text notifications to claimants	Encrypted Tablespaces Hardware encryption of volumes
Enrollment Manager	Yes	Yes	FIRST_NAME LAST_NAME	Required to identify students for Enrollment Manager	Encrypted Tablespaces Hardware encryption of volumes
Payment (6)	No	Yes	VA_PERSON_ID VA_FILE_NUMBER SOCIAL_SECURITY_NUMBER FIRST_NAME LAST_NAME MIDDLE_NAME DATE_OF_BIRTH DATE_OF_DEATH TRANSFEROR_DATE_OF_DEATH GENDER	Required for claimant benefit generation	Encrypted Tablespaces Hardware encryption of volumes
RHSSO	No	Yes	FIRST_NAME LAST_NAME MIDDLE_NAME EMAIL_ADDRESS	Required for user authentication to the system	Encrypted Tablespaces Hardware encryption of volumes
Splunk (1)	No	Yes	VA_PERSON_ID VA_FILE_NUMBER FIRST_NAME LAST_NAME MIDDLE_NAME EMAIL_ADDRESS IP_ADDRESS	Required for audit logging	Hardware encryption of volumes
User Access	Yes	Yes	FIRST_NAME LAST_NAME MIDDLE_NAME EMAIL_ADDRESS USERID USERNAME/EMAIL	Required for user authentication to the system	Encrypted Tablespaces Hardware encryption of volumes
Vets (5)	No	Yes	VA_PERSON_ID VA_FILE_NUMBER FIRST_NAME LAST_NAME MIDDLE_NAME EMAIL_ADDRESS	Required for claimant benefit generation	Encrypted Tablespaces Hardware encryption of volumes

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?

Data is input into the Digital GI Bill through the following entities.

- Chapter33:
  - Veteran Claims Examiners (VA Employees)
- Enrollment Manager
  - State Approving Agencies (VA Contractors)
  - School Certifying Officials (Unaffiliated)
- System Interfaces
  - IAM
  - VA.gov
  - VA DoD Identity Repository
  - Benefits Delivery Network
  - EDU PITC Web Applications
- Veteran Input
  - SMS confirmation of class registration

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.

Digital GI Bill is a claims processing and automation system used by VA employees and contractors to facilitate educational benefit claim processing for individuals. Data necessary to make claims determination is sourced from various trusted VA entities, this data cannot be obtained from the individual as the system must evaluate and verify the integrity of the individuals claim.

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

Identity and Access Management (IAM) – Data is collected via IAM to uniquely identify and authorize users to role within the DGI.

VA DoD Identity Repository (VDR) – The VA/DoD Repository data is used to prepopulate claimant service data to facilitate claims adjudication. AD data provides authoritative user service history from the DOD and is a key component in calculating entitlement authorizations.

Benefits Delivery Network (BDN) – BDN provides authoritative information on claims payments for DGI that is needed to determine payment history and to facilitate future payments.

Common Security Service (CSS) – CorpDB CSS provides interface to central VA database for the sensitivity level.

Corporate Database (CRP) – CRP provides interface to store historical and archival information.

Veterans-Facing Services Platform-Va.gov (VFSP-Va.gov) – VA.gov, a web-based application(s) that allows the submission of various VA forms electronically to provide access to the DGI provided services. DGI interface with the Government email server and VA Twilio to communicate with stakeholders.

VA Profile – VAPRO provides single source of truth for Veteran data across all VA systems. Synchronizes name, phone/email, address, military personnel data, awards, disability ratings. Veterans Benefits Management Systems (VBMS) Cloud Assessing – VBMS eFolder to access Education claim-related documents that have been processed by the Government's scanning vendor.

BIP Assessing (BIP) – Enterprise Management of Payments, Workload, and Reporting (eMPWR-VA) for processing of VBA EDU payments and overpayments, offsets, withholdings and updates to budgetary data and General Ledger (GL). Additionally, DGI will receive transaction success/failure status from eMPWR-VA to allow for resubmission of failed transactions.

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?

The following are methods in which the information identified in 1.2 are collected:

- **IAM** data exchanged through Web Service calls
- **VDR** data exchanged through Web Service calls
- **BDN** data exchanged through Web Service calls
- **CSS** data exchanged through Web Service calls
- **CRP** data exchanged through Web Service calls
- **VA.gov** data exchanged through Web Service calls
- **VA Profile** data exchanged through Web Service calls

- **BIP Assessing** – eMPWR-VA data exchanged through Web Service calls

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?

N/A

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.

The DGI does not collect information directly from the Veterans. It relies on the systems that collect and provide the data to check accuracy of the information. The application enforces some input validation measures (e.g.Valid SSN entry), but it's primarily the application end users that are responsible for validating information for accuracy along with built in application checks for input validation.

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?

N/A

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

VCE end users are responsible for validating information for accuracy along with built in application checks for input validation.

SORN 58VA21/22/28 states authority for DGI: Title 10 U.S.C. chapters 106a, 510, 1606 and 1607 and title 38, U.S.C., § 501(a) and Chapters 3, 11, 13, 15, 18, 19, 21, 23, 30, 31, 32, 33, 34, 35, 36, 37, 39, 51, 53, 55 and 77. Title 5 U.S.C. 5514 (https://www.oprm.va.gov/privacy/systems_of_records.aspx).
2021-24372.pdf (govinfo.gov)

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

Consider the specific data elements collected and discuss the potential privacy risks and what steps, if any are currently being taken to mitigate those identified risks. (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: The DGI collects Personally Identifiable Information (PII) and other sensitive information. If this information was breached or accidentally released to inappropriate parties or the public, it could result in financial, personal, and/or emotional harm to the individuals whose information is contained in the system.

Mitigation: The system adheres to information security requirements instituted be the VA Office of Information Technology (OIT). All employees/contractors with access to Veterans' information are required to complete the VA Privacy and Information Security Awareness training and Rules of Behavior annually. The VA only collects the information necessary to identify the parties involved in an incident, identify potential issues and concerns, and offer assistance to the affected parties.

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**
VA_PERSON_ID	Individual Identifier	Not Used
VA_FILE_NUMBER	VA_FILE_NUMBER – Individual Identifier	Not Used
SOCIAL_SECURITY_NUMBER	Individual Identifier	Not Used
FIRST_NAME	Individual Identifier	Not Used
LAST_NAME	Individual Identifier	Not Used
MIDDLE_NAME	Individual Identifier	Not Used
DATE_OF_BIRTH	Used for entitlement benefit calculations in the system	Not Used
DATE_OF_DEATH	Used for entitlement benefit calculations in the system	Not Used
GENDER	Used for entitlement benefit calculations in the system	Not Used
ADDRESS_LINE_1	Used for communications	Not Used
ADDRESS_LINE_2	Used for communications	Not Used
ADDRESS_LINE_3	Used for communications	Not Used
CITY	Used for communications	Not Used
STATE_CODE_KEY	Used for communications	Not Used
ZIPCODE	Used for communications	Not Used
PRIMARY_PHONE_NUMBER	Used for communications with the user	Used
SECONDARY_PHONE_NUMBER	Used for communications with the user	Not Used
Home_PHONE	Used for communications with the user	Not Used
MOBILE_PHONE	Used for communications with the user	Not Used
EMAIL_ADDRESS	Used for communications with the user	Not Used
BRANCH_OF_SERVICE	Used for entitlement benefit calculations in the system	Not Used
BASD_DATE (Basic Active Service Date)	Used for entitlement benefit calculations in the system	Not Used
CHARACTER_OF_SERVICE	Used for entitlement benefit calculations in the system	Not Used
REASON_FOR_SEPARATION	Used for entitlement benefit calculations in the system	Not Used
POWER_OF_ATTORNEY_NAME	Used for communication	Not Used
TRANSFEROR_DATE_OF_DEATH	Used for entitlement benefit calculations in the system	Not Used
USERID	Individual Identifier	Not Used
USERNAME/EMAIL	Used for communications with the user	Not Used
CURRENT_FIRST_NAME	Individual Identifier	Not Used
CURRENT_LAST_NAME	Individual Identifier	Not Used
PREVIOUS_FIRST_NAME	Individual Identifier	Not Used
PREVIOUS_LAST_NAME	Individual Identifier	Not Used
Direct Deposit Account Type	Used to update payment information for claimant services	Not Used

Direct Deposit Account Number	Used to update payment information for claimant services	Not Used
Direct Deposit Routing Number	Used to update payment information for claimant services	Not Used
DEP_CHILD_DOB	Individual Identifier	Not Used
DEP_CHILD_NAME	Individual Identifier	Not Used
DEP_CHILD_STAT	Used for entitlement benefit calculations in the system	Not Used
DISAB_EXT_DATE	Used for entitlement benefit calculations in the system	Not Used
SPOUSE_NAME	Individual Identifier	Not Used

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?

Application data inputs are checked to enforce applicable format and acceptable range compliance consistent with DGI requirements such as required fields. Data is checked by system audits, as well as, manual verifications, for example, data such as annual Basic Allowance for Housing (BAH) rates update. The system must collect all the data types/fields to verify the correct Veteran is receiving the correct benefits he/she is entitled to.

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.

Should new data be made available that was either previously unutilized or is new to the individual record, the existing Veteran record would be updated to incorporate that new data. Any newly derived information may be used to make additional determinations about the individual claimant record. One such example would be claim payment adjustments due to housing payment calculation logic changes in support of newly introduced Government legislation. Such determinations undergo rigorous consultation and thorough testing with Education Services Business sponsors in accordance with DGI system agile practices to support any necessary user interface, data model, application data processing, etc. updates to assure desired results based on the recently introduced legislation policy.

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?

Both data in transit and data at rest are protected by FIPS validated encryption algorithms. All data within DGI is encrypted at rest using AWS KMS. Data in transit utilizes standard encrypted protocols such as SSH and TLS (TLS 1.2). Insecure ports and protocols are blocked at the firewall.

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

While all data is protected to the same technical standard (encryption at rest and in transit) there are additional handling measures utilized with social security numbers such as minimizing the use of SSNs wherever possible using internal unique identifiers, ensuring redaction of SSN data from any system audits, ensuring SSN data is not utilized where it may be accessed insecurely such as within a URI query string, and other security considerations as the use case dictates.

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

1. The information with each applicant is categorized in accordance with FIPS 199 and NIST SP 800-60. As part of the categorization any PII is identified.
2. The VA has policies which direct and guide the activities and processes performed by the VA. The policies are periodically reviewed to ensure completeness and applicability.
3. The NIST SP 800-53 controls are selected based on the categorization. The controls provide protection for veteran PII while developed or stored by an application or IT system, least privilege, stored offsite.
4. Internal protection is managed by access controls such as user IDs and passwords, authentication, awareness and training, auditing, and internal network controls. Remote protection is provided by remote access control, authenticator management, audit, and encrypted transmission.

2.4 <u>PRIVACY IMPACT ASSESSMENT: Use of the information.</u>

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?

> The SORN defines the information collected from veterans, use of the information, and how the information is accessed and stored. The information collected is used for determining a veteran's benefits, such as compensation or education.

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

> The security controls for the DGI cover 17 security areas with regard to protecting the confidentiality, integrity, and availability of VA information systems and the information processed, stored, and transmitted by those systems. The security areas include access control; awareness and training; audit and accountability; certification, accreditation, and security assessments; configuration management; contingency planning; identification and authentication; incident response; maintenance; media protection; physical and environmental protection; planning; personnel security; risk assessment; systems and services acquisition; system and communications protection; and system and information integrity. The DGI team has implemented the required security controls based on the tailoring guidance of NIST Special Publication 800-53 Rev 4 and VA directives or handbooks. VA Records Management Policy VA 6300.1, VA 6500 HB, National Rules of Behavior (ROB), and VA 6502.1, VA6502.3, VA 6502.4 Privacy Policies govern how veterans' information is used, stored, and protected.

2.4c Does access require manager approval?

Backend users requesting access require manager and ISO approval for access to DGI systems with sensitive data. Users of the application all have roles based on job requirements and sensitivity of data that is needed to complete job functions.

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

Only approved backend users can access the DGI system. All user activity is monitored in accordance with DGI audit and accountability controls. Only approved application users can see veteran's information that matches their job role/level. This is enforced via a Security Assertion Markup Language (SAML) assertion that follows the user throughout the application.

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

As per VA guidelines, the DGI Information System Owner (ISO) in conjunction with the Information System Security Officer (ISSO) and Privacy Officer (PO) monitor and audit privacy controls continuously.

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*

VA_PERSON_ID – Individual Identifier
VA_FILE_NUMBER – Individual Identifier
SOCIAL_SECURITY_NUMBER – Individual Identifier
FIRST_NAME – Individual Identifier
LAST_NAME – Individual Identifier
MIDDLE_NAME – Individual Identifier
DATE_OF_BIRTH – Used for entitlement benefit calculations in the system
DATE_OF_DEATH – Used for entitlement benefit calculations in the system
GENDER – Used for entitlement benefit calculations in the system
ADDRESS_LINE_1 – Used for communications
ADDRESS_LINE_2 – Used for communications
ADDRESS_LINE_3 – Used for communications
CITY – Used for communications
STATE_CODE_KEY – Used for communications
ZIPCODE – Used for communications
PRIMARY_PHONE_NUMBER – Used for communications with the user
SECONDARY_PHONE_NUMBER – Used for communications with the user
HOME_PHONE – Used for communications with the user
MOBILE_PHONE – Used for communications with the user
EMAIL_ADDRESS – Used for communications with the user
BRANCH_OF_SERVICE – Used for entitlement benefit calculations in the system
BASD_DATE (Basic Active Service Date) – Used for entitlement benefit calculations in the system
CHARACTER_OF_SERVICE – Used for entitlement benefit calculations in the system
REASON_FOR_SEPARATION – Used for entitlement benefit calculations in the system
POWER_OF_ATTORNEY_NAME – Used for communication
TRANSFEROR_DATE_OF_DEATH – Used for entitlement benefit calculations in the system
USERID – Individual Identifier
USERNAME/EMAIL – Used for communications with the user
CURRENT_FIRST_NAME – Individual Identifier
CURRENT_LAST_NAME – Individual Identifier

PREVIOUS_FIRST_NAME – Individual Identifier
PREVIOUS_LAST_NAME – Individual Identifier
DIRECT DEPOSIT ACCOUNT TYPE – Used to update payment information for claimant services
DIRECT DEPOSIT ACCOUNT NUMBER – Used to update payment information for claimant services
DIRECT DEPOSIT ROUTING NUMBER – Used to update payment information for claimant services
DEP_CHILD_DOB – Individual Identifier
DEP_CHILD_NAME – Individual Identifier
DEP_CHILD_STAT – Used for entitlement benefit calculations in the system
DISAB_EXT_DATE – Used for entitlement benefit calculations in the system
SPOUSE_NAME – Individual Identifier

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.*

The SORN will be updated to include Cloud specific information regarding retention and retrieval of information. Until such time it is put in place DGI will maintain all records.

SORN 58VA21/22/28 states:
Compensation, pension, and vocational rehabilitation claims file folders are retained at the servicing regional office until they are inactive for three years, after which they are transferred to the Records Management Center (RMC) for the life of the veteran. At the death of the veteran, these records are sent to the Federal Records Center (FRC), and maintained by the FRC for 75 years, and thereafter, destroyed. Some claims files folders are electronically imaged, in which case, the electronic file folder is maintained in the same manner as the claims file folder.
Once a file is electronically imaged and accepted by VA, its paper contents (with the exception of service treatment records and official legal documents), are destroyed in accordance with Records Control Schedule VB–1 Part 1 Section XIII, as authorized by the National Archives and Records Administration (NARA) of the United States.

Vocational Rehabilitation counseling records are maintained until the exhaustion of a veteran’s maximum entitlement or upon the exceeding of a veteran’s delimiting date of eligibility (generally, ten or twelve years from discharge or release from active duty), whichever occurs first, and then destroyed. Automated storage media containing temporary working information are retained until a claim is decided, and then destroyed. All other automated storage media are retained and disposed of in accordance with disposition authorization approved by NARA. Education electronic file folders are retained at the servicing Regional Processing Office. Education folders may be destroyed in accordance with the times set forth in the Veterans Benefits Administration Records Management, Records Control Schedule VB–1, Part 1, Section VII, as authorized by NARA.

Employee productivity records are maintained for two years after which they are destroyed by shredding or burning. File information for CAIVRS is provided to HUD by VA on magnetic tape. After information from the tapes has been read into the computer the tapes are returned to VA for updating. HUD does not keep separate copies of the tapes.

Audit event data such as system access logs are retained for 365 days. Any trace level data will be retained for the duration of its usefulness to facilitate system operations and diagnostics, not exceed 365 days.

The System meets the requirements of the 36 CFR XII – National Archives and Records Administration, SUBCHAPTER B – Records Management, which prescribes policies for Federal agencies' records management programs relating to records creation and maintenance, adequate documentation, and proper records disposition. The regulations in this subchapter implement the provisions of 44 U.S.C. Chapters 21, 29, 31, and 33. These regulations apply to Federal agencies as defined in 36 C.F.R. § 1220.18.

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?

Yes

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

DGI uses the Veterans Benefits Administration Records Management, Records Control Schedule (RCS) VB–1, Part 1, Section VII approved by NARA.
Admin20, Rcs, Part 1, Introduction (va.gov)
https://www.benefits.va.gov/WARMS/docs/regs/RCS_I.doc

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.

DGI will adhere to VBA Letter 20-21-04, Records and Information Management, VA 6300 Records and Information Management when the records are authorized for destruction (or upon system decommission), will be carried out in as detailed in NIST SP800-88 Rev 1 Section 2.6 Use of Cryptography and Cryptographic Erase.

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.

The DGI application only uses PII within the Production (PRD) and Integration (INT) environments. The Production (PRD) environment is composed of production and preproduction instances, meanwhile the Integration (INT) environment is composed of User Acceptance Test (UAT) and Performance Test (PERF) instances. The Integration environments uses the same information found in the Production environment. This is to test if system and application changes would affect performance or stability within the Production environment. Both PRD and INT environments are held to the Moderate impact baseline. The Production environment does not conduct testing. Development (DEV) and Integrated Verification and Validation (IVV) instances contain generic sanitized data.

<u>3.6 PRIVACY IMPACT ASSESSMENT: Retention of information</u>

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:

<u>Principle of Minimization:</u> *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?*

<u>Principle of Data Quality and Integrity:</u> *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: There is a risk that the information maintained by DGI could be retained for longer than is necessary to fulfill the VA mission. Records held longer than required are at greater risk of being unintentionally released or breached.

Mitigation: To mitigate the risk posed by information retention, DGI adheres to the VA RCS schedules for each category or data it maintains. When the retention data is reached for a record, the system owner will carefully dispose of the data by the determined method as described in question 3.4. VA Handbook 6500 contains the policies and responsibilities that VA components are required to follow to manage data breaches, including detection, correlation, notification, remediation, and reporting.

All environments containing PII follows the requirements of a Moderate level system detailed in the VA 6500 Handbook. This ensures that all data is protected based on the level of information contained within the system.

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***
Identity Access Management Office of Information Security (OIT) **Identity and Access Management Assessing (IAM)**	DGI Interface with IAM for user provisioning/credentialing. DGI interface with VA Master Person Index (**VA MPI**) for claimant/beneficiary identification and contact information. MPI is the new predominant data repository.	VA_PERSON_ID SOCIAL_SECURITY_NUMBER FIRST_NAME LAST_NAME MIDDLE_NAME DATE_OF_BIRTH GENDER EMAIL_ADDRESS	Hypertext Transfer Protocol Secure (HTTPS)
Data and Analytics Veterans Experience Office (VEO) **VA DoD Identity Repository (VDR)**	DGI Interface with **VDR** to obtain Military Service information. VDR data is used to prepopulate claimant service data to facilitate claims adjudication. It provides user service history from the DOD and is a key component in calculating entitlement authorizations.	VA_PERSON_ID VA_FILE_NUMBER SOCIAL_SECURITY_NUMBER FIRST_NAME LAST_NAME MIDDLE_NAME DATE_OF_BIRTH DATE_OF_DEATH GENDER ADDRESS_LINE_1 ADDRESS_LINE_2 ADDRESS_LINE_3 CITY STATE_CODE_KEY ZIPCODE PRIMARY_PHONE_NUMBER SECONDARY_PHONE_NUMBER EMAIL_ADDRESS BRANCH_OF_SERVICE BASD_DATE CHARACTER_OF_SERVICE REASON_FOR_SEPARATION	HTTPS
Education Veteran Readiness and Employment Education Service (VBA) **Benefits Delivery Network (BDN)**	DGI interface with **BDN**, a system used to pay education benefits. BDN (ECAP, NEWMAN) provides authoritative information on claims payments for DGI that is needed to determine	VA_PERSON_ID VA_FILE_NUMBER SOCIAL_SECURITY_NUMBER FIRST_NAME LAST_NAME MIDDLE_NAME DATE_OF_BIRTH DATE_OF_DEATH	HTTPS

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***
	payment history and to facilitate future payments. **VRAP** (part of Chapter 30 on the BDN): To support VRAP benefits that have not been transferred to Chapter 33 and remaining 1607 beneficiaries, the Contractor shall provide a means for VA to manually review, manage workload, and finalize claims that cannot be processed through standard, approved, processes to include claims that are not ingested through automated intake services.	GENDER ADDRESS_LINE_1 ADDRESS_LINE_2 ADDRESS_LINE_3 CITY STATE_CODE_KEY ZIPCODE PRIMARY_PHONE_NUMBER SECONDARY_PHONE_NUMBER EMAIL_ADDRESS BRANCH_OF_SERVICE BASD_DATE CHARACTER_OF_SERVICE REASON_FOR_SEPARATION DEP_CHILD_DOB DEP_CHILD_NAME DEP_CHILD_STAT DISAB_EXT_DATE NAME_ADDRESS SPOUSE_NAME	
Benefits Integration and Administration Office of Business Integration (VBA) **VBA Corporate Infrastructure (CRP)** and **Common Security Services (CSS) –** falls under Benefits Enterprise Platform (**BEP)**	DGI interface with Corporate Database **(CRP)** to store historical and archival information. And for sensitivity level.	VA_PERSON_ID VA_FILE_NUMBER SOCIAL_SECURITY_NUMBER FIRST_NAME LAST_NAME MIDDLE_NAME DATE_OF_BIRTH DATE_OF_DEATH GENDER ADDRESS_LINE_1 ADDRESS_LINE_2 ADDRESS_LINE_3 CITY STATE_CODE_KEY ZIPCODE PRIMARY_PHONE_NUMBER SECONDARY_PHONE_NUMBER EMAIL_ADDRESS BRANCH_OF_SERVICE BASD_DATE CHARACTER_OF_SERVICE REASON_FOR_SEPARATION	HTTPS
IT Infrastructure Operations and Services (OIT)	Austin Information Technology Center (AITC) hosts on-premise information systems in support of the Veterans	FIRST_NAME LAST_NAME MIDDLE_NAME ADDRESS_LINE_1 ADDRESS_LINE_2	SFTP

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***
Austin Information Technology Center (AITC) To interface with Pinnacle Data Systems (PDS) / Government Printing Office (GPO) for all Education Service printing.	Experience. DGI interface with AITC to interface with the Pinnacle Data Systems (PDS) / **Government Printing Office (GPO)** for all Education Service printing.	ADDRESS_LINE_3 CITY STATE_CODE_KEY ZIPCODE	
Benefits Integration and Administration Performance Analysis and Integrity (VBA) **Performance Analysis and Integrity Reporting (PA&I) Business Intelligence (VD3)**	DGI interface with the Data Warehouse / Performance, Analysis, and Integrity to provide Business Analytics and Reporting to VBA Office. The VBA PA&I receives real-time status updates and other information on the claims and backlog inventory data from DGI.	VA_PERSON_ID VA_FILE_NUMBER SOCIAL_SECURITY_NUMBER FIRST_NAME LAST_NAME MIDDLE_NAME DATE_OF_BIRTH DATE_OF_DEATH GENDER ADDRESS_LINE_1 ADDRESS_LINE_2 ADDRESS_LINE_3 CITY STATE_CODE_KEY ZIPCODE PRIMARY_PHONE_NUMBER SECONDARY_PHONE_NUMBER EMAIL_ADDRESS BRANCH_OF_SERVICE BASD_DATE CHARACTER_OF_SERVICE REASON_FOR_SEPARATION	SFTP
Digital Experience Veterans Experience Office (VEO) **Veterans-Facing Services Platform-Va.gov (VFSP-Va.gov)**	DGI interface with **VA.gov**, a web-based application(s) that allows the submission of various VA forms electronically to provide access to the DGI provided services. DGI interface with the Government email server to communicate with stakeholders.	VA_PERSON_ID VA_FILE_NUMBER SOCIAL_SECURITY_NUMBER FIRST_NAME LAST_NAME MIDDLE_NAME DATE_OF_BIRTH DATE_OF_DEATH GENDER ADDRESS_LINE_1 ADDRESS_LINE_2 ADDRESS_LINE_3 CITY STATE_CODE_KEY ZIPCODE PRIMARY_PHONE_NUMBER	HTTPS

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***
		SECONDARY_PHONE_NUMBER EMAIL_ADDRESS BRANCH_OF_SERVICE BASD_DATE CHARACTER_OF_SERVICE REASON_FOR_SEPARATION Direct Deposit Account Type Direct Deposit Account Number Direct Deposit Routing Number	
Data and Analytics Veterans Experience Office (VEO) **VA Profile**	**VAPRO** provides single source of truth for Veteran data across all VA systems. Synchronizes name, phone/email, address, military personnel data, awards, disability ratings.	FIRST_NAME LAST_NAME MIDDLE_NAME ADDRESS_LINE_1 ADDRESS_LINE_2 ADDRESS_LINE_3 CITY STATE_CODE_KEY ZIPCODE PRIMARY_PHONE_NUMBER SECONDARY_PHONE_NUMBER EMAIL_ADDRESS BRANCH_OF_SERVICE BASD_DATE CHARACTER_OF_SERVICE REASON_FOR_SEPARATION	HTTPS
Education Veteran Readiness and Employment Office of Financial Management (VBA) **BIP Assessing (BIP)** Salesforce – Enterprise Management of Payments Workload, and Reporting. Child under BIP. **(eMPWR-VA)**	DGI interface with Enterprise Management of Payments, Workload, and Reporting **(eMPWR-VA)** for processing of VBA EDU payments and budgetary data and General Ledger (GL). Additionally, DGI will receive transaction success/failure status from eMPWR-VA to allow for resubmission of failed transactions, overpayments, offsets, withholdings and updates	VA_PERSON_ID VA_FILE_NUMBER SOCIAL_SECURITY_NUMBER FIRST_NAME LAST_NAME MIDDLE_NAME DATE_OF_BIRTH DATE_OF_DEATH GENDER ADDRESS_LINE_1 ADDRESS_LINE_2 ADDRESS_LINE_3 CITY STATE_CODE_KEY ZIPCODE PRIMARY_PHONE_NUMBER SECONDARY_PHONE_NUMBER EMAIL_ADDRESS BRANCH_OF_SERVICE BASD_DATE CHARACTER_OF_SERVICE REASON_FOR_SEPARATION	HTTPS

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***
Cybersecurity Office of Information Security (OIT) **CSOC Vulnerability Scanning System Assessing (CSOC VSS)**	The CSOC provides vulnerability management system scanning and VA log aggregation.	IP_ADDRESS	HTTPS

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

Discuss the privacy risks associated with the sharing of information within the Department and what steps, if any, are currently being taken to mitigate those identified risks. (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: The privacy risk associate with maintaining PII is that sharing data within the Department of Veterans' Affairs could happen, and that the data may be disclosed to individuals who do not require access and heightens the threat of the information being misused.

Mitigation: All employees/contractors with access to Veterans' information are required to complete the VA Privacy and Information Security Awareness training and Rules of Behavior annually.

Information is shared in accordance with VA Handbook 6500

The principle of need-to-know is strictly adhered by DGI personnel. Only personnel with a clear business purpose are allowed access to the system and the information contained within. This action adheres to the idea of least privilege and need to know found in the VA 6500 Handbook. Access to the DGI Production application requires a VA issued identity assertion via SSOi or SSOe along with the proper IAM permissions for login.

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***
Amazon Web Services (AWS)	The majority of DGI systems and information are hosted in AWS GovCloud	VA_PERSON_ID VA_FILE_NUMBER SOCIAL_SECURITY_NUMBER FIRST_NAME LAST_NAME MIDDLE_NAME DATE_OF_BIRTH DATE_OF_DEATH GENDER ADDRESS_LINE_1 ADDRESS_LINE_2 ADDRESS_LINE_3	SORN 58VA21/22/28 Routine Use #6 and Purchasing Contract Agreement between AFS	HTTPS SFTP

		CITY STATE_CODE_KEY ZIPCODE PRIMARY_PHONE_NUMBER SECONDARY_PHONE_NUMBER EMAIL_ADDRESS BRANCH_OF_SERVICE BASD_DATE CHARACTER_OF_SERVICE REASON_FOR_SEPARATION IP_ADDRESS USERID USERNAME/EMAIL AWS operates the underlying infrastructure that the majority of DGI components run on top of.	and Third-Party Vendor	
Mulesoft	Provides API integration services with the VA and the DGI managed service.	VA_PERSON_ID VA_FILE_NUMBER SOCIAL_SECURITY_NUMBER FIRST_NAME LAST_NAME MIDDLE_NAME DATE_OF_BIRTH DATE_OF_DEATH GENDER ADDRESS_LINE_1 ADDRESS_LINE_2 ADDRESS_LINE_3 CITY STATE_CODE_KEY ZIPCODE PRIMARY_PHONE_NUMBER SECONDARY_PHONE_NUMBER EMAIL_ADDRESS BRANCH_OF_SERVICE BASD_DATE CHARACTER_OF_SERVICE REASON_FOR_SEPARATION IP_ADDRESS USERID USERNAME/EMAIL While Mulesoft processes all data types noted, only IP_ADDRESS is retained within the component.	SORN 58VA21/22/28 Routine Use #6 and Purchasing Contract Agreement between AFS and Third-Party Vendor	HTTPS SFTP
DynaTrace	Provides application performance monitoring and tracing.	IP_ADDRESS USERID USERNAME/EMAIL Application logs for Performance tracing.	SORN 58VA21/22/28 Routine Use #6 and Purchasing Contract Agreement between AFS	HTTPS

			and Third-Party Vendor	
Duo Federal	Cisco Duo Federal provides multi-factor authentication services for internal platform components.	FIRST_NAME LAST_NAME MIDDLE_NAME PRIMARY_PHONE_NUMBER IP_ADDRESS USERID USERNAME/EMAIL This is for DGI Staff accounts on the system, not personal information. No veteran information is synced with Duo.	SORN 58VA21/22/28 Routine Use #6 and Purchasing Contract Agreement between AFS and Third-Party Vendor	HTTPS
Accenture XDR	Performs monitoring of application and system access logs for tracing of security event audits.	IP_ADDRESS USERID USERNAME/EMAIL Application and system access logs for tracing of security event audits.	SORN 58VA21/22/28 Routine Use #6 and Purchasing Contract Agreement between AFS and Third-Party Vendor	HTTPS
SentinelOne	Provides Antivirus/Antimalware and endpoint Extended Detection and Response services.	IP_ADDRESS USERID USERNAME/EMAIL Antivirus and endpoint Extended Detection and Response service.	SORN 58VA21/22/28 Routine Use #6 and Purchasing Contract Agreement between AFS and Third-Party Vendor	HTTPS
Twilio	Provides SMS capabilities to DGI for user communications. such as enrollment verification check-ins.	PRIMARY_PHONE_NUMBER Connection for end user communication.	SORN 58VA21/22/28 Routine Use #6 and Purchasing Contract Agreement between AFS and Third-Party Vendor	HTTPS

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

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: The privacy risk associated with maintaining PII is that sharing data outside of the Department of Veteran's Affairs could increase the risk that data may be disclosed to individuals who do not require access and heightens the threat of the information being misused.

Mitigation: The principle of least privilege is strictly adhered to by the DGI personnel. Only authorized personnel that have authenticated to the system are allowed access to the system and the information contained within the system. Security controls from the VA 6500 Handbook are implemented and constantly reviewed to determine if changes to information sharing need to be changed.

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.

DGI pulls data from other systems. It also obtains veteran information in the following way.

1. Veterans / dependents utilize VA.gov to access the My Education Benefits module to submit for benefits eligibility, verifications etc. This data is then synced over to DGIB via a webservice.
2. Veterans / dependents are sent text messages to provide YES/NO feedback on whether they have been enrolled in an eligible program for the prior month. Veteran SMS responses of YES/NO are directly processed by DGIB which involves NO PII.

The Department of Veterans Affairs does provide public notice that the system does exist. This notice is provided in 2 ways.

3. The System of Records Notice (SORN) "Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA"; (SORN 58VA21/22/28) 86FR 61858

   SORN 58VA21/22/28 are located at:

   [2021-24372.pdf (govinfo.gov)]

4. This Privacy Impact Assessment (PIA) also serves as notice of the DGI. As required by the eGovernment Act of 2002, Pub.L. 107–347 §208(b)(1)(B)(iii), the Department of Veterans Affairs "after completion of the [PIA] under clause (ii), make the privacy impact assessment publicly available through the website of the agency, publication in the Federal Register, or other means".

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

DGI pulls data from other systems. It also obtains veteran information in the following way.

1. Veterans / dependents utilize VA.gov to access the My Education Benefits module to submit for benefits eligibility, verifications etc. This data is then synced over to DGIB via a webservice.
2. Veterans / dependents are sent text messages to provide YES/NO feedback on whether they have been enrolled in an eligible program for the prior month. Veteran SMS responses of YES/NO are directly processed by DGIB which involves NO PII.

The Department of Veterans Affairs does provide public notice that the system does exist. This notice is provided in 2 ways.

3. The System of Records Notice (SORN) "Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA"; (SORN 58VA21/22/28) 86FR 61858

   SORN 58VA21/22/28 are located at:

   [2021-24372.pdf (govinfo.gov)]

4. This Privacy Impact Assessment (PIA) also serves as notice of the DGI. As required by the eGovernment Act of 2002, Pub.L. 107–347 §208(b)(1)(B)(iii), the Department of Veterans Affairs "after completion of the [PIA] under clause (ii), make the privacy impact assessment publicly available through the website of the agency, publication in the Federal Register, or other means".

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.

N/A

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.

All information collected from other government sources and systems listed in section 1.2. Depending on the information required, some data collection is mandatory while others are voluntary. Failure to provide information may result in denial of compensation and pension benefits. Veterans and their family or guardian (spouse, children, parents, grandparents, etc.) may not decline or request their information not be included as part to determine eligibility and entitlement for VA compensation and pension benefits and designate a guardian to manage the VA compensation and pension benefits.

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.

Depending on the information required, some data collection is mandatory while others are voluntary. Failure to provide information may result in denial of compensation and pension benefits. Veterans and their family or guardian (spouse, children, parents, grandparents, etc.) may not decline or request their information not be included as part to determine eligibility and entitlement for VA compensation and pension benefits and designate a guardian to manage the VA compensation and pension benefits.

6.4 <u>PRIVACY IMPACT ASSESSMENT: Notice</u>

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: There is a risk that individuals may not been given notice of the DGI or the data contained in that system.

Mitigation: The VA mitigates this risk by providing the public with two forms of notice that the system exists, as discussed in detail in question 6.1, including the Privacy Act statement and a System of Record Notice (SORN).

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.***

Individuals wishing to obtain more information about access, redress and record correction of the Digital GI Platform should contact the Department of Veteran's Affairs regional office as directed in the System of Record Notice (SORN) 58VA21/22/28 SORN and can be found at: 2021-24372.pdf (govinfo.gov)

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)?

N/A

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?

N/A

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.

Individuals wishing to obtain more information about access, redress and record correction of the Digital GI Platform should contact the Department of Veteran's Affairs regional office as directed in the System of Record Notice (SORN) 58VA21/22/28 SORN and can be found at: 2021-24372.pdf (govinfo.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.

Individuals wishing to obtain more information about access, redress and record correction of the Digital GI Platform should contact the Department of Veteran's Affairs regional office as directed in the System of Record Notice (SORN) 58VA21/22/28 SORN and can be found at: 2021-24372.pdf (govinfo.gov)

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

Redress is the process by which an individual gains access to his or her records and seeks corrections or amendments to those records. Redress may be provided through the Privacy Act and Freedom of Information Act (FOIA), and also by other processes specific to a program, system, or group of systems. ***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.

Formal redress is provided in SORN 58VA21/22/28 SORN and can be found at: 2021-24372.pdf (govinfo.gov)

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

Mitigation: By publishing this PIA, and the applicable SORN, the VA makes the public aware of the unique status of applications and evidence files, such as those stored on the Virtual VA platform. Furthermore, this document and the SORN provide the point of contact for members of the public who have questions or concerns about applications and evidence files.

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?

Per VA Directive and Handbook 6330, every 5 years the Office of Information Technology (OIT) develops, disseminates, and reviews/updates a formal, documented policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; along with formal, documented procedures to facilitate the implementation of the control policy and associated controls.

VA documents and monitors individual information system security training activities including basic security awareness training and specific information system security trainin g; and retains individual training records for 7 years. This documentation and monitoring are performed using VA's Talent Management System (TMS).

For the DGI, VA Identity and Access Management (IAM) provides the user management of all DGI application users. This control requires each person to have a unique username, account updates, and account disabling.

VA employees or contractors submit an IAM request by choosing the Chapter 33 application, select an applicable user role, facility, and access level. VCE and other application users do not have access to the underlying infrastructure such as operating systems or databases. This access is only given to system administrators.

DGI Platform administrators request access to underlying systems by submitting a VA 9957 form to the system owner. This form includes type of access (i.e. database, server, windows, etc.), create, modify, or delete user, and access requested (i.e. read, write, execute permissions, specific environments). 9957 forms are then sent to the system owner for review and accepted if the system owner agrees a user needs access.

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?

N/A

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.

VCE and other application users do not have access to the underlying infrastructure such as operating systems or databases. This access is only given to DGI system administrators. Only VCE roles can edit veteran work products.

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.

Contractor access is verified through VA personnel before access is granted to any contractor. Contracts and contractor access are reviewed annually at a minimum. Elevated privileges are reviewed quarterly. The contractors who provide support to the system are required to complete annual VA Privacy and Information Security and Rules of behavior training via TMS. All contractors are cleared using the VA background investigation process and must obtain the appropriate background investigation for their role. Contractors with systems administrative access are required to complete additional role-based training prior to gaining system administrator access.

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.

Personnel that will be accessing information systems must read and acknowledge their receipt and acceptance of the VA National Rules of Behavior (ROB) prior to gaining access to any VA information system or sensitive information. The rules are included as part of the VA Privacy and Information Security Awareness and Rules of Behavior (VA10176) training which all personnel must complete via the VA's Talent Management System (TMS). After the user's initial acceptance of the Rules, the user must re-affirm their acceptance annually as part of the security awareness training. Acceptance is obtained via electronic acknowledgment and is tracked through the TMS system. VA users with access to protected health information must complete mandatory HIPAA Privacy training annually in TMS.

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

8.4a If Yes, provide:

1. *The Security Plan Status:* Approved
2. *The System Security Plan Status Date:* 08 August 2023
3. *The Authorization Status:* Authorized to Operate (ATO)
4. *The Authorization Date:* 23 October 2023
5. *The Authorization Termination Date:* 23 October 2024
6. *The Risk Review Completion Date:* 20 October 2023
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.***

N/A

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)*

The DGI system consists of cloud technology from various vendors such as AWS GovCloud (FedRAMP High), Accenture XDR (FedRAMP Moderate), Mulesoft (FedRAMP Moderate), SentinelOne (FedRAMP Moderate), and Duo Federal (FedRAMP Moderate). DGI being a managed service will be assessed and authorized with all component included in the assessment. DGI system utilizes a combination of SaaS, PaaS and IaaS cloud models internally within the managed service provided to the VA. AWS GovCloud (IaaS), Accenture XDR (SaaS), Mulesoft (PaaS), SentinelOne (SaaS), and Duo Federal (SaaS).

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.*

All data and business rules related to Veterans and service provision remain the property of the VA, and that processes be in place for VA to access / maintain copies of this data and business rules as required by the Department.

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.

While VA application metadata, audits, etc. will be controlled by DGI and owned by the VA, DGI CSPs will collect ancillary data necessary to provide the backend cloud service such as billing metrics and audit events when interacting with the CSP management plane. Such ancillary data will be owned by the respective CSP.

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.

The Contractor shall manage aspects of interfacing/configuring automation/AI with VBA systems. This includes complying with the security requirements in VA Handbook 6500 and referenced NIST standards to safeguard the data of Veterans who depend upon VA. Security compliance includes obtaining and maintaining an agency-level Authority to Operate (ATO) which shall prevent the Contractor from processing transactions in production systems until complete.

Contract: VA118-16-D-1013 36C10D21N0007
Accenture T4NG-0557 DGIB Attachment B PWS

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).

N/A

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

ID	Privacy Controls
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.

MARVIS HARVEY Digitally signed by MARVIS HARVEY
Date: 2024.04.15 07:54:56 -05'00'

Privacy Officer, Marvis Harvey

BOBBI DEE BEGAY Digitally signed by BOBBI DEE BEGAY
Date: 2024.04.15 09:47:17 -06'00'

Information System Security Officer, Bobbi Begay

RILEY ROSS Digitally signed by RILEY ROSS
Date: 2024.04.15 16:40:32 -04'00'

Information System Owner, Riley Ross

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).

https://www.va.gov/privacy-policy/

The Department of Veterans Affairs provide public notice that the system does exist. This notice is provided in 2 ways.

1. The System of Records Notice (SORN) "Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA"; (SORN 58VA21/22/28) 86FR 61858

   SORN 58VA21/22/28 are located at:
2. This Privacy Impact Assessment (PIA) also serves as notice of the DGI. As required by the eGovernment Act of 2002, Pub.L. 107–347 §208(b)(1)(B)(iii), the Department of Veterans Affairs "after completion of the [PIA] under clause (ii), make the privacy impact assessment publicly available through the website of the agency, publication in the Federal Register, or other means".

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