Privacy Impact Assessment for the VA IT System called:

Veterans Information Solution (VIS)

Veterans Relationship Management (VRM)

Veterans Benefit Administration (VBA)

Date PIA submitted for review:

May 06, 2022

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Gina Siefert	gina.siefert@va.gov	(202) 632-7861
Information System Security Officer (ISSO)	Eric Abraham	Eric.Abraham@va.gov	(512) 326-7422
Information System Owner	Alexander Torres	Alexander.Torres@va.gov	(703) 300-5511

Abstract

The abstract provides the simplest explanation for "what does the system do?" and will be published online to accompany the PIA link.

Veterans Information Solution (VIS) is an intranet web-based application that provides a consolidated view of comprehensive eligibility utilization data from across the Veterans Benefit Administration (VBA). VIS provides access to profile, service, rating and award information and benefits payments data. VIS also correlates profile, service, education, and miscellaneous information.

Overview

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

- *The IT system name and the name of the program office that owns the IT system.*
- *The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission.*
- *Indicate the ownership or control of the IT system or project.*
- *The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.*
- *A general description of the information in the IT system and the purpose for collecting this information.*
- *Any information sharing conducted by the IT system. A general description of the modules and subsystems, where relevant, and their functions.*
- *Whether the system is operated in more than one site, and if so, a description of how use of the system and PII is maintained consistently in all sites and if the same controls are used across sites.*
- *A citation of the legal authority to operate the IT system.*
- *Whether the completion of this PIA will result in circumstances that require changes to business processes*
- *Whether the completion of this PIA could potentially result in technology changes*
- *If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval? If the system is using cloud technology, does the SORN for the system cover cloud usage or storage?*

The Veterans Information Solution (VIS) is a web-based, query application that provides a consolidated view of comprehensive eligibility and benefits utilization data from across the Veterans Benefit Administration (VBA) and the Department of Defense (DoD). The VIS system supports customer groups throughout the entire VA.

VIS enables authorized users to search records and retrieve information on the Veteran's or Service member's profile or military history; on certain education benefits; and information on compensation and disability pension ratings and awards and on dependents included in those awards. VIS accesses

VA/Department of Defense Identity Repository (VADIR), a database replicated from Defense Manpower Data Center (DMDC).

VIS provides access to disability rating and award, benefits provided, benefit payment information from the VBA Corporate Database, and beneficiary information from VBA's Beneficiary Identification and Locator System (BIRLS, now part of VBA Corporate DB) for Veterans and Service members.

VIS also provides Claimant entitlement information from Benefits Delivery Network (BDN).

Medals and Awards Web Service (MAWS) is a DMDC web service that VIS utilizes for Veteran Medals and Awards information.

The VIS system itself stores no data; it is only a front-end user interface that accesses other data repositories. Data on approximately 13 million Veterans is stored within the databases that VIS accesses. VIS performs no information sharing. It displays information extracted from other VA databases that the operator uses to support the Veteran and their dependents as needed.

The legal authority to operate system is Title 38, U.S.C., Part II, Chapters 11, 13, 15, 17 - 19, and 23. The Secretary of Veterans Affairs established these guidelines pursuant to the authorities in and requirements of Title 38, United States Code, section 81 11 (38 U.S.C. 5811 I), titled "Sharing of Department of Veterans Affairs and Department of Defense Health Care Resources." and the authorities contained under Title 10, United States Code, section 1104 (10 U.S.C.5 1104), titled "Sharing of Resources with the Department of Veterans Affairs," which incorporates Title 31, United States Code, section 1535 (31 U.S.C. 51 535), titled "Agency Agreements," also known as the "Economy Act." These guidelines assist in the implementation of these statutes. Completion of this PIA will not result in technology changes. VIS does not use cloud technology.

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.

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

☒ Name
☒ Social Security Number
☒ Date of Birth
☒ Mother's Maiden Name
☒ Personal Mailing Address
☒ Personal Phone Number(s)
☒ Personal Fax Number
☒ Personal Email Address
☒ Emergency Contact Information (Name, Phone Number, etc. of a different individual)
☐ Financial Account Information

☐ Health Insurance Beneficiary Numbers Account numbers
☐ Certificate/License numbers
☐ Vehicle License Plate Number
☐ Internet Protocol (IP) Address Numbers
☐ Current Medications
☐ Previous Medical Records
☒ Race/Ethnicity
☐ Tax Identification Number
☐ Medical Record Number
☐ Gender

☐ Integration Control Number (ICN)
☐ Military History/Service Connection
☐ Next of Kin
☒ Other Unique Identifying Information (list below)

Military history (DD- 214) and service periods,
combat/deployment periods,
National Guard/Reserves service periods,
service number (pre-SSN),
compensation & pension,
VA- & service-provided education,
member's maiden name,
deployment-related information,
supporting Veteran Service Organization (VSO),
Survivor Benefit Program participation,
special pay periods (hazardous duty incentive, imminent danger, combat zone tax exclusion),
disability rating information,
benefits award history,
Beneficiary information
BIRLS Service

PII Mapping of Components

The Veterans Information Solution (VIS) does not collect/store any PII information. It is a read-only application, that accesses servers owned by other information systems. Those systems are listed in the PTA as the IT systems that VIS connects, receives, or shares PII with another internal VA organization. VIS connects to, and receives data from, those other information system servers, and shares (displays) the information with the user performing the query from the terminal.

PII Mapped to Components

Note: Due to the PIA being a public facing document, please do not include the server names in the table.

PII Mapped to Components

Database Name of the information system collecting/storing PII	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
VDRP	Yes	Yes	Military Service History, VA_ID PN_1ST_NM PN_MID_NM PN_LST_NM PN_CDNCY_NM PN_ID PN_ID_TYP_CD DUP_ID PN_XR_TYP_CD PN_XR_DT SSA_VER_STAT_CD PN_ID_CHNG_RSN_CD PN_BRTH_DT PN_DTH_DT PN_DTH_CD RACE_CD ETHNC_NAT_ORIG_CD EDU_LVL_CD EDU_LVL_DT PRIOR_PN_1ST_NM PRIOR_PN_LST_NM MRTL_STAT_CD SPN_VA_ID VA_ID PNA_RSN_CD PNA_BGN_DT PNA_END_DT PNA_ERSN_CD MA_LN1_TX MA_LN2_TX MA_CITY_NM MA_ST_CD MA_PR_ZIP_CD + MA_PR_ZIPX_CD MA_CTRY_CD MA_ISO_A3_CTRY_CD MA_TYP_CD MA_DT MA_MAINT_DT MA_MAINT_SRC_CD TNUM_TYP_CD TNUM_CD	Permit authorized users to view Veteran information	Internal VA secure web (HTTPS)

			LST_UPD_DT EMA_TX EMA_USE_PRTY_CD EMA_DLVRY_QL_CD EMA_SRC_CD EMA_PMSN_CD ORG_CD PNL_CAT_CD PNL_SEG_ID PNL_BGN_DT PNL_TERM_DT PNL_TRSN_CD PNL_PE_DT PEDC_CD SVC_CD UNIF_SVC_INIT_ ENT_DT MIL_ACC_SRC_CD ENL_ASVC_AGMT_ YR_QY INIT_ENTRY_TRN_ END_DT BSC_ACT_SVC_DT PNL_BDSRC_CD PNL_TDSRC_CD LST_UPD_DT CHAR_SVC_CD NARR_RSN_SEP_CD PNLST_CHNG_TYP_CD REENL_ELIG_CD ISVC_SEP_CD ISVC_REENL_CD PAY_PLN_CD PG_CD PG_DT RANK_CD DOD_OCC_CD SVC_OCC_CD SVC_OCC_DT OCC_TYP_CD MILPAY_IND_CD MILPAY_BGN_DT MILPAY_TERM_DT CMBT_ZN_CTRY_CD CMBT_ZN_ISO_A3_ CTRY_CD DPLY_BGN_DT DPLY_TERM_DT DPLY_TRSN_CD DPLY_PROJ_CD DPLY_CTRY_CD DPLY_ISO_A3_ CTRY_CD DPLY_LOC_ MBW_CD DPLY_LOC_BGN_DT DPLY_LOC_ TERM_DT DPLY_LOC_ TRSN_CD PRPLHRT_AWRD_DT PRPLHRT_AWRD_ SVC_CD DOD_DSBL_PCT_CD PNL_DSBL_EXT_CD PNL_DSBL_PCT_CD RET_TYP_CD GROSS_AWARD_ AMT NET_AWARD_DT SUSPNS_SGMNT_ IND VET_SSN_NBR COMBND_DEGREE_ DSBLTY DSBL_DTR_DT DSBL_TYP_CD PAYEE_NBR PAYEE_SSN GRAS_BGN_DT		

			GRAS_TERM_DT GRAS_PE_DT GRAS_TRSN_CD PNL_CAT_CD CHAR_SVC_CD NARR_RSN_SEP_CD GRAS_PROJ_CD GRAS_STATUTE_CD SPN_VA_ID VA_ID VA_SPN_REL_CD CHAMPVA_EFF_DT CHAMPVA_EXP_DT CHAMPVA_ERSN_CD MGAD_LOSS_ CAT_CD PGIB_ LOSS_CAT_CD SR_LOSS_TYP_CD MGAD_LOSS_ CAT_CD PGIB_ LOSS_CAT_CD SR_LOSS_TYP_CD INCN_CD INCN_ELIG_BGN_DT INCN_ELIG_END_DT INCN_TRSN_CD SPN_VA_ID TRFBL_SPN_ AGMT_CD TRFBL_SPN_ AGMT_DT TRFBL_PGM_ELCT_ TYP_CD TRFBL_SVC_REP_ VER_CD TRFBL_SVC_REP_ VER_DT TRFBL_SVC_REP_ VER_RSN_CD TRFBL_OBLG_PE_DT SPN_VA_ID VA_ID TRFBL_DEP_ BGN_DT TRFBL_DEP_PE_DT TRFBL_DEP_ PEDC_CD TRFBL_DEP_ TERM_DT TRFBL_DEP_ TRSN_CD TRFBL_DEP_MN_QY MGIB_PGM_TYP_CD MGIB_KI_RT_CD MGAD_PRIOR_ ENRL_CD MGIB_KI_BAS_CD MGAD_BPR_AMT OVEB_ENTL_CD MGAD_ENRL_ BAS_CD MGAD_ENRL_ ACTN_CD MGAD_ENRL_ ACTN_DT MGAD_OBLG_ YRS_CD MGSR_BGN_DT MGSR_BBNF_ SVC2_DT MGAD_CTRB_AM MGAD_CTRB_DT MGAD_LOSS_ CAT_CD ENL_ASVC_AGMT_ YR_QY MGSR_AGRM_ YRS_CD MIL_ACC_SRC_CD MGIB_PGM_TYP_CD MGIB_BNF_TYP_CD MGSR_STAT_CD MGSR_STAT_ EFF_DT MGSR_OBLG_SVC_MTHS_QY MGSR_TRSN_CD REAP_QUAL_ BGN_DT REAP_STAT_CD REAP_STAT_EFF_DT REAP_TRSN_CD		

| | | | REAP_CTRB_AM
REAP_CTRB_DT
REAP_CTRB_ STAT_CD
VA_EDU_PGM_ TYP_CD
VA_EDU_ENTL_ MN_QY
VA_EDU_ENTL_ END_DT
VA_EDU_PGM_ LST_UPD_DT
VA_PN_TYP_CD
VA_EDU_ELCT_CD
SPN_VA_ID
VA_EDU_PGM_ TYP_CD
VA_BNF_PMT_ STAT_CD
VA_BNF_PMT_ MN_QY
VA_BNF_PMT_AM
VA_RCR_PMT_AM
VA_PMT_PCT_CD
VA_BNF_LST_ PMT_DT
VA_BNF_PMT_ LST_UPD_DT
VA_KBNF_PMT_ SRC_CD
SPN_VA_ID
VA_HSNG_PMT_AM
VA_BOOK_PMT_AM
VA_BOOK_PMT_DT
VA_RURAL_ PMT_AM
VA_RURAL_PMT_DT
VA_TUTR_PMT_AM
VA_TUTR_PMT_DT
VA_YRP_PMT_AM
VA_YRP_PMT_DT
VA_LIC_CTFCN_ PMT_AM
VA_LIC_CTFCN_ PMT_DT
VA_NATL_EXM_ PMT_AM
VA_NATL_EXM_ PMT_DT
VA_CH30_RFND_ PMT_AM
VA_CH30_RFND_ PMT_DT
VA_HSNG_LSUM_ PMT_AM
VA_HSNG_LSUM_ PMT_DT | | |
| VBA1 | Yes | Yes | Disability rating and award, benefits provided, benefit payment information,
FIRST_NM
MIDDLE_NM
LAST_NM
SUFFIX_NM
SSN_NBR
BRTHDY_DT
FILE_NBR
DEATH_DT
BEGIN_DT
CLAIM_RCVD_DT
PAYEE_TYPE_CD
AWARD_CURNT_ STATUS_CD
SC_COMBND_PCT_ NBR
AMT
PTCPNT_DPOSIT_ACNT_ID
SCHOOL_CHILD_NBR
TRSURY_ADDRS_ONE_TXT
TRSURY_ADDRS_TWO_TXT
TRSURY_ADDRS_ THREE_TXT
TRSURY_ADDRS_ FOUR_TXT
TRSURY_ADDRS_ FIVE_TXT
TRSURY_ADDRS_ SIX_TXT
ZIP_PREFIX_NBR
ZIP_FIRST_SUFFIX_ NBR | Permit authorized users to view Veteran information | Internal VA secure web (HTTPS) |

			EFCTV_DT		
			NM		
			ENTLMT_TYPE_CD		
			MINOR_CHLDRN_NBR		
			HELP_CHILD_NBR		
			SCHOOL_CHILD_NBR		
			PARENT_NBR		
			SPOUSE_TXT		
			GROSS_AMT		
			NET_AMT		
			IVAP_AMT		
			GROSS_AMT		
			INDVDL_UNEMPL_IND		
			SMC_TYPE_CD		
			HOSP_SMC_TYPE_CD		
			DGNSTC_TYPE_CD		
			DGNSTC_TXT		

1.2 What are the sources of the information in the system?

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

Describe why information from sources other than the individual is required. For example, if a program's system is using data from a commercial aggregator of information or data taken from public Web sites, state the fact that this is where the information is coming from and then in question 1.3 indicate why the system is using this source of data.

If the system creates information (for example, a score, analysis, or report), list the system as a source of information.
This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

VIS accesses VA/Department of Defense Identity Repository (VADIR), a database replicated from Defense Manpower Data Center (DMDC).
VIS provides access to disability rating and award, benefits provided, benefit payment information from the VBA Corporate Database for Veterans and Service members, Benefits Delivery Network (BDN) for claimant entitlement information, and DMDC MAWS Web Service for Medals and Awards information.

1.3 How is the information collected?

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

If the information is collected on a form and is subject to the Paperwork Reduction Act, give the form's OMB control number and the agency form number.
This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

VIS extracts the information it displays from VA databases and has no contact with subjects. VIS obtains the Medals and Awards information from DMDC through the MAWS web service and has no contact with subjects.

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

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

If the system checks for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract.
This question is related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.

Information is not entered into VIS; all information retrieved through VIS is assumed correct. In the event it is determined a piece of retrieved information is incorrect, then the Veteran or VSO will have to request correction with the host database.

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

The System of record Notice (SORN) Veterans Information Solution (VIS)—
VA has been rescinded and is no longer in effect.
The Secretary of Veterans Affairs established these guidelines pursuant to the authorities in and requirements of Title 38, United States Code, section 81 11 (38 U.S.C. 5811 I), titled "Sharing of Department of Veterans Affairs and Department of Defense Health Care Resources." and the authorities contained under Title 10, United States Code, section 1104 (10 U.S.C.5 1104), titled "Sharing of Resources with the Department of Veterans Affairs," which incorporates Title 31, United States Code, section 1535 (31 U.S.C. 51 535), titled "Agency Agreements," also known as the "Economy Act." These guidelines assist in the implementation of these statutes.

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

Consider the specific data elements collected and discuss the potential privacy risks and what steps, if any are currently being taken to mitigate those identified risks.

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

Principle of Purpose Specification: Explain how the collection ties with the purpose of the underlying mission of the organization and its enabling authority.

Principle of Minimization: Is the information directly relevant and necessary to accomplish the specific purposes of the program?

Principle of Individual Participation: Does the program, to the extent possible and practical, collect information directly from the individual?

Principle of Data Quality and Integrity: Are there policies and procedures for VA to ensure that personally identifiable information is accurate, complete, and current?
This question is related to privacy control AR-1, Governance and Privacy Program, and AR-2, Privacy Impact and Risk Assessment.

Follow the format below when entering your risk assessment:
Privacy Risk: There is a risk a report which contains PII is printed and removed from a controlled facility.

Mitigation: VIS does not maintain data. Only individuals who have access (approved by their leadership) can access Veteran and dependent information as required by their role.
Users are trained in their responsibilities to protect and secure protected information at all times. All employees acknowledge and accept their responsibilities in safeguarding sensitive information through the VA Rules of Behavior, which also details the appropriate disciplinary action that can be expected for violating VA security policies. VIS has security controls in place that follow VA 6500 Handbook and NIST SP800-53.

Section 2. Uses of the Information

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

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

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

Name: Used to identify Veteran.
Social Security Number: Used to verify the identity of the Veteran.

Date of Birth: Used to verify the identity of the Veteran.
Mother's Maiden Name: Used to verify the identity of the Veteran.
Mailing Address: Used to verify the identity of the Veteran.
Zip Code: Used to verify the identity of the Veteran.
Phone Number: Used to verify the identity of the Veteran.
Fax Number: Used to verify the identity of the Veteran.
Email Address: Used to verify the identity of the Veteran.
Emergency Contact Information: Used to verify the identity of the Veteran.
Race/Ethnicity: Used to identify Veteran patient records.
The following information is used to accurately identify the Veteran for benefits processing: Military history (DD-214) and service periods, combat/deployment periods, National Guard/Reserves service periods, service number (pre-SSN), compensation & pension, VA- & service-provided education, member's maiden name, deployment-related information, supporting Veteran Service Organization (VSO), Survivor Benefit Program participation, special pay periods (hazardous duty incentive, imminent danger, combat zone tax exclusion), disability rating information, and benefits award history.

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

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

If the system creates or makes available new or previously unutilized information about an individual, explain what will be done with the newly derived information. Will it be placed in the individual's existing record? Will a new record be created? Will any action be taken against or for the individual identified because of the newly derived data? If a new record is created, will the newly created information be accessible to Government employees who make determinations about the individual? If so, explain fully under which circumstances and by whom that information will be used.
This question is related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information

The system performs no data analysis; only requested information is displayed.

2.3 How is the information in the system secured?
> *2.3a What measures are in place to protect data in transit and at rest?*
> Audit log records user identification information along with related activity information such as search type (by name, SSN, or file number), search parameters, and veteran identification data. Veterans' identification data is encrypted by the key stored in WebLogic Keystore and cannot be viewed without decrypting it.

2.3b If the system is collecting, processing, or retaining Social Security Numbers, are there additional protections in place to protect SSNs?
The Veterans Information Solution (VIS) is a read-only application and only displays information. It does not collect or process PII information and displays the last 4 of the SSN except for 2 screens when the entire SSN is also displayed.
The Veterans Information Solution (VIS) does not collect and store any PHI information.

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

There is no PHI data in VIS.VIS application code is periodically scanned and security vulnerabilities are fixed. Server infrastructure is regularly patched with updates per VA standards. These practices ensure proper security procedures are in place. VIS application is internal facing and users outside the VA firewall cannot access it. Supervisors requesting access for their employees are responsible to ensure sensitive information is appropriately safeguarded and used responsibly.

This question is related to security and privacy controls SC-9, Transmission Confidentiality, and SC-28, Protection of Information at Rest

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information. How is access to the PII determined? Are criteria, procedures, controls, and responsibilities regarding access documented? Does access require manager approval? Is access to the PII being monitored, tracked, or recorded? Who is responsible for assuring safeguards for the PII?

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

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

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

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

Add answer here:

All VA employees and contractors are required to protect personal, health, and VA sensitive information, and document this understanding on the VA Rules of Behavior. VIS accounts are generated through the VA account creation process and are described in detail in the VIS System Security Plan. All users of the system are authenticated through Windows active directory, and all workflow activities are audited through the server logs.

VA Records Management Policy and the VA Rules of Behavior govern how Veterans' information is used, stored, and protected.

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

VIS retains information within the operator's search queue only for the life of that session. When the user logs out, the workstation cache is flushed, and no information is retained by VIS. The information displayed may include Name, Social Security Number, Date of Birth, Mailing Address, Zip Code, Phone Numbers, Fax numbers, Email Addresses, Race/ethnicity, Military history (DD-214) and service periods, combat/deployment periods, National Guard/Reserves service periods, service number (pre-SSN), compensation & pension, VA- & service-provided education, member's maiden name, deployment-related information, supporting Veteran Service Organization (VSO), Survivor Benefit Program participation, special pay periods (hazardous duty incentive, imminent danger, combat zone tax exclusion), disability rating information, and benefits award history and Emergency Contact Information (Name, Phone Number, of a different individual).

3.2 How long is information retained?

In some cases VA may choose to retain files in active status and archive them after a certain period of time. State active file retention periods, as well as archived records, in number of years, for the information and record types. For example, financial data held within your system may have a different retention period than medical records or education records held within your system, please be sure to list each of these retention periods. If the system is using cloud technology, will it be following the NARA approved retention length and schedule?

The VA records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented.
This question is related to privacy control DM-2, Data Retention and Disposal.

The VIS application does not retain information, it only keeps information within the operator's search queue until the next search is initiated, or until logout. When the user logs out, the workstation cache is flushed.
No information is retained by VIS.

3.3 Has the retention schedule been approved by the VA records office and the National Archives and Records Administration (NARA)? If so please indicate the name of the records retention schedule.

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

The VIS application electronically stores personal information on Veterans only long enough to fulfill a user's request for information; once the user's request is fulfilled, the data is expunged from the system.

3.4 What are the procedures for the elimination of SPI?

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

The VIS Application does not retain Veteran's personal data in the application system. VIS queries three data systems (VADIR, VBA Corporate Database [now includes BIRLS information], BDN) to meet user requests for data; once the user request has been satisfied, the data is expunged from the system.

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

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

Only test data is used in the lower environments for research, testing and training. There is no real PII information in these environments.

3.6 <u>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.

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

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

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

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

Follow the format below:
Privacy Risk: VIS does not retain data. Therefore, the only risk is a report containing PII is printed and removed from a controlled facility.

Mitigation: VIS does not maintain data. Only individuals who have access (approved by their leadership) can access Veteran and dependent information as required by their role.
Users are always trained in their responsibilities to protect and secure protected information. All employees acknowledge and accept their responsibilities in safeguarding sensitive information through the VA Rules of Behavior, which also details the appropriate disciplinary action that can be expected for violating VA security policies.

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*
VA/DoD Identity Repository (VDR)	Permit authorized users to view Veteran information	Military service history	Internal VA secure web (HTTPS)
VBA Corporate Database	Permit authorized users to view Veteran information	Disability rating and award, benefits provided, benefit Payment information	Internal VA secure web (HTTPS)

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

Discuss the privacy risks associated with the sharing of information within the Department and what steps, if any, are currently being taken to mitigate those identified risks.
This question is related to privacy control UL-1, Internal Use.

Follow the format below:
<u>Privacy Risk:</u> The privacy risk associated with maintaining PII is that sharing data within the Department of Veterans' Affairs could happen and the data may be disclosed to individuals who do not require access, which heightens the threat of the information being misused.

<u>Mitigation:</u> The principle of need-to-know is strictly adhered by the Perceptive Reach Integrated Reach Database personnel. Only personnel with a clear business purpose are allowed access to the system and the information contained within.

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*

Defense Manpower Data Center (DMDC) MAWS web service	For Veteran Medals & Awards Information	Award Description Award Date Award From Date Award To Date Service Code Source Code Device Description	MOU	DMDC MAWS web service

5.2 **PRIVACY IMPACT ASSESSMENT: External sharing and disclosure**

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

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

Discuss how the sharing of information outside of the Department is compatible with the stated purpose and use of the original collection.

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

Follow the format below:
Privacy Risk: There is a risk of data compromise at the external location.

Mitigation: A Memorandum of Understanding (MOU) exists for DMDC (MAWS) and outlines the protective measures necessary to ensure the proper confidentiality, availability, and integrity of the stored data. These agreements are reviewed annually.

Section 6. Notice

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

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

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

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

Describe how the notice provided for the collection of information is adequate to inform those affected by the system that their information has been collected and is being used appropriately. Provide information on any notice provided on forms or on Web sites associated with the collection. This question is related to privacy control TR-1, Privacy Notice, and TR-2, System of Records Notices and Privacy Act Statements, and TR-3, Dissemination of Privacy Program Information.

The System of record Notice (SORN) Veterans Information Solution (VIS)—
VA has been rescinded and is no longer in effect.
The Secretary of Veterans Affairs established these guidelines pursuant to the authorities in and requirements of Title 38, United States Code, section 81 11 (38 U.S.C. 5811 I), titled "Sharing of Department of Veterans Affairs and Department of Defense Health Care Resources." and the authorities contained under Title 10, United States Code, section 1104 (10 U.S.C.5 1104), titled "Sharing of Resources with the Department of Veterans Affairs," which incorporates Title 31, United States Code, section 1535 (31 U.S.C. 51 535), titled "Agency Agreements," also known as the "Economy Act." These guidelines assist in the implementation of these statutes.

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

VIS does not collect the information contained in the system directly from individuals. The information is pulled from other VA systems and the MAWS web service. Any notice provided would be made through those applications.

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

VIS does not collect the information contained in the system directly from individuals. The information is pulled from other VA systems and the MAWS web service. Any notice provided would be made through those applications

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.

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 a Veteran may not know their information may be entered into a long-term records storage system.

Mitigation: The Veteran is informed during their transition from military service that the information they provided will be stored in systems the VA uses to adjudicate and grant/deny benefits, and additional documents will be included in those collections and protected accordingly.

Section 7. Access, Redress, and Correction

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

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

Cite any procedures or regulations your program has in place that allow access to information. These procedures, at a minimum, should include the agency's FOIA/Privacy Act practices, but may also include additional access provisions. For example, if your program has a customer satisfaction unit, that information, along with phone and email contact information, should be listed in this section in addition to the agency's procedures. See 5 CFR 294 and the VA FOIA Web page at http://www.foia.va.gov/ to obtain information about FOIA points of contact and information about agency FOIA processes.

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

If the system is not a Privacy Act system, please explain what procedures and regulations are in place that covers an individual gaining access to his or her information.
This question is related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.

Access to the information displayed by VIS would be in accordance with the databases VIS accesses and would be covered in those databases PIAs

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.

Correction to the information displayed by VIS would be in accordance with the databases VIS accesses and would be covered in those databases PIAs.

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.

VIS does not collect the information contained in the system directly from individuals. The information is pulled from other VA systems and the MAWS web service. Any notice provided would be made through those applications.

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

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

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

There is no formal redress for records displayed within the VIS; however, Veterans and other beneficiaries may contact their supporting VA regional office or VHA center to learn how to access, correct, or contest their information. VIS does not store any information.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction
Discuss what risks there currently are related to the Department's access, redress, and correction policies and procedures for this system and what, if any, steps have been taken to mitigate those

risks. For example, if a project does not allow individual access, the risk of inaccurate data needs to be discussed in light of the purpose of the project. For example, providing access to ongoing law enforcement activities could negatively impact the program's effectiveness because the individuals involved might change their behavior.

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

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

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

Follow the format below:
Privacy Risk: There is a risk a Veteran may not know how to obtain access to their records or how to request corrections to their records.

Mitigation: If it is determined a piece of retrieved information is incorrect, then the Veteran or VSO will have to request correction with the host database.

Section 8. Technical Access and Security

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

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

Describe the process by which an individual receives access to the system.

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

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

This question is related to privacy control AR-7, Privacy-Enhanced System Design and Development.

Account requests are approved by the regional VIS coordinator, and only authorized registered individuals are granted access to the system. End users are required to follow a standard registration process managed by the Common Security Employee Manager (CSEM) system. The VA-Form 20- 8824E must be submitted to local ISO for each user. The submitting official must complete all appropriate boxes on the form identifying a specific set of user permissions. Upon

complete approval of the signed form, the form is submitted and entered into CSEM, where the information updates the Common Security Service (CSS) database to create a user profile. The applicant is then registered as a system user and assigned a specific VIS user role in accordance with previously established CSS templates. All VIS users are listed in the CSS, which also serves as a documented repository of the user's sensitivity (access) level.

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.

Regular users of VIS are authorized VA and contractor employees. There are contractor system administration personnel within the Austin Information Technology Center (AITC) who maintain the server hardware and software but are not privileged users of the VIS system itself. Contracts are reviewed annually by the VIS application's Program Manager, Information System Owner, Information Owner, Contract Officer, Privacy Officer, and the Contracting Officer's Technical Representative. Contractor personnel accessing information systems must read and acknowledge their receipt and acceptance of the VA Contractor's ROB (for AITC technicians) prior to gaining access to any VA information system or sensitive information. The ROB includes non-disclosure and confidentiality agreements.

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 accessing information systems must read and acknowledge their receipt and acceptance of the VA National Rules of Behavior (ROB) or VA Contractor's ROB (for AITC technicians) prior to gaining access to any VA information system or sensitive information. The rules are included as part of the security awareness training which all personnel must complete via the VA's Talent Management System (TMS). After the user's initial acceptance of the Rules, the user must reaffirm their acceptance annually as part of the security awareness training. Acceptance is obtained via electronic acknowledgment and is tracked through the TMS system. All VA employees must complete annual Privacy and Security training.

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

If Yes, provide:

1. *The Security Plan Status,* VIS Security plan has been completed
2. *The Security Plan Status Date,* Signed on December 28, 2021
3. *The Authorization Status,* VIS has a 6month ATO
4. *The Authorization Date,* March 4, 2022
5. *The Authorization Termination Date,* August 31, 2022
6. *The Risk Review Completion Date*, September 14, 2021
7. *The FIPS 199 classification of the system* HIGH.

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

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

Veterans Information Solution received an ATO with conditions on 31-August-2022 for 182 days. The system has a FIPS 199 classification of High.

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).

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.

VIS does not use cloud technology.

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

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

VIS does not use cloud technology.

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

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

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

VIS does not use cloud technology.

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

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

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

VIS does not use cloud technology.

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

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

VIS does not use the RPA technology.

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

ID	Privacy Controls
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.

_____

Privacy Officer, Gina Siefert

_____

Information System Security Officer, Eric Abraham

_____

Information System Owner, Alexander Torres

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).