The completion of Veterans Affairs Privacy Impact Assessments (PIAs) is mandated for any rulemaking, program, system, or practice that collects or uses PII under the authority of the E-government Act of 2002 (44 U.S.C. § 208(b)) and VA Directive 6508, Implementation of Privacy Threshold Analysis and Privacy Impact Assessment.

The PIA is designed to identify risk associated with the use of PII by a system, program, project or practice, and to ensure that vital data stewardship issues are addressed for all phases of the System Development Life Cycle (SDLC) of IT systems. It also ensures that privacy protections are built into an IT system during its development cycle. By regularly assessing privacy concerns during the development process, VA ensures that proponents of a program or technology have taken its potential privacy impact into account from the beginning. The PIA also serves to help identify what level of security risk is associated with a program or technology. In turn, this allows the Department to properly manage the security requirements under the Federal Information Security Management Act (FISMA).


Please note that the E-government Act of 2002 requires that a PIA be made available to the public. In order to comply with this requirement PIA will be published online for the general public to view. When completing this document please use simple, straight-forward language, avoid overly technical terminology, and write out acronyms the first time you use them to ensure that the document can be read and understood by the general public.
Privacy Impact Assessment for the VA IT System called:

Des Moines RO VBA GSS

Date PIA completed:
09/28/2017

VA System Contacts:

<table>
<thead>
<tr>
<th>Name</th>
<th>E-mail</th>
<th>Phone Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy Officer</td>
<td>Stacey Lampe</td>
<td><a href="mailto:Stacey.lampe@va.gov">Stacey.lampe@va.gov</a></td>
</tr>
<tr>
<td>Information Security</td>
<td>Terrence Rausch</td>
<td><a href="mailto:Terrence.rausch@va.gov">Terrence.rausch@va.gov</a></td>
</tr>
<tr>
<td>Officer</td>
<td>System Owner</td>
<td>Mary Barley</td>
</tr>
</tbody>
</table>
Abstract

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

The Des Moines Regional Office General Support System (GSS) is a general support system. However, no major applications are supported by this system. The Des Moines RO GSS simply hosts the client portion of each client-server major application. The Regional Offices are a separate system from the VA EWAN (Enterprise Wide Area Network) and are managed separately. All Veterans’ Benefit Administration (VBA) Regional Offices are configured in the following way. The local area network consists of a Cisco WSC6506-E layer 3 routing core switch. That switch performs all the routing for the VBA Regional Office. The VBA is responsible for and maintains the LAN (Local Area Network) system. The VBA does not have a WAN (Wide Area Network) system. All VBA Regional Office LANs connect to the VA Enterprise WAN which is a separate system maintained by NSOC (Network and Security Operations Center) with the system owner being Mary Barley.

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.
- The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.
- If your system is a regional GSS, VistA, or LAN, include a list of the hospitals/medical centers, or other regional offices that fall under your system. Additionally, what region is the system under?
- A general description of the information in the IT system.
- 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?
- Does the system use cloud technology? 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.
- Does a contract with Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII?
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 is the magnitude of harm if privacy related data is disclosed, intentionally or unintentionally? Would the reputation of the CSP or its customers (VA) be affected?

The VBA Regional Offices, under the direction of the Veterans’ Benefits Act (38 U.S. Code Chapter 77), provide benefits and services to eligible veterans, their families, and beneficiaries. These benefits and services include compensation, pension, education, insurance, loan guaranty, and vocational rehabilitation and counseling. VBA activities address the receipt, processing, tracking, and disposition of veterans’ applications for benefits, services, and requests for assistance. VBA activities also address the general administration of legislated benefit programs.

To help fulfill the responsibilities of the VBA, the Des Moines Regional Office uses a GSS to assist in serving 1,000,000 to 9,999,999 veterans and their dependents. The GSS consists of file servers, routers, printers, and networked personal computers which allow for the processing and storage of data necessary for carrying out VBA functions. The Des Moines Regional Office GSS does not directly host or maintain any major VA systems or applications. Any data stored on the system is the result of employees directly storing or maintaining data, such as Excel Spreadsheets or Word Documents, on the network. Although the majority of veteran data is stored in a central database not located at this facility, during the processing of benefits, it is often necessary for employees to store files containing personal information on the network. This is done for a variety of reasons to include but not limited to temporary storage while working a case, for reference purposes, or to assist in case management. Any potential records created, maintained, or stored on the Des Moines Regional Office GSS are governed by Veterans Affairs System of Record Notice (VA SORN) Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA, SORN 58VA21/22/28 (July 19, 2012).

The Des Moines Regional VBA Office GSS connects directly to the VA Enterprise wide-area network, maintained by the VA Network Security Operations Center (NSOC). This allows select users at the Des Moines Veterans Affairs Medical Center (VAMC) limited access to a web based Hospital Inquiry database known as WebHINQ, and Veterans Information Solution (VIS), which are used to verify Veteran’s eligibility for benefits, and Veterans Benefits Management System (VBMS), which is used to process Veteran’s disability claims. Users with the Iowa Department of Veterans Services, Vietnam Veterans of America, Disabled American, American Legion, Veterans of Foreign Wars, Military Order of the Purple Heart, and Paralyzed Veterans of America Veterans are provided read only access to Control of Veteran’s Records (COVERS), Share, a Microsoft Windows®-based application which is utilized by the Regional Offices (RO) to access the Beneficiary Inquiry Records Locator System (BIRLS), Compensation and Pension (C&P) Master Records, Pending Issue File (PIF), Payment History File (PHF), Corporate database, Social Security Administration, and COVERS records.

Share provides a single computing system with data sources located on different databases in multiple locations. Veterans Appeals Control and Locator System (VACOLS), Virtual VA, VBMS and Modern Award Processing (MAP-D), an application to help perform proper claims development. However, no major applications are supported by this system. All the major applications are supported and located at various sites throughout the United States, and the local general support system (GSS) only accesses the applications through the network. The Des Moines RO GSS simply hosts the client portion of each client-server major application. The Regional Offices are a separate system from the Veterans Affairs Enterprise Wide Area Network (VA EWAN) and are managed separately. The Veteran’s claims information is either entered
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? Are the types of information collected, used, maintained, and/or shared specified in its Privacy Notices?

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 the VA Handbook 6500 (http://www.va.gov/vapubs/viewPublication.asp?Pub_ID=638&FType=2, published Sept. 2012, Appendix A).

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.

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
- Mailing Address
- Zip Code
- Phone Number(s)
- Fax Number
- 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

Other personal information accessible through the GSS includes: bank account information, employment history, gross income and net worth information.

The record, or information contained in the record, may include
- identifying information (e.g., name, address, social security number);
• military service and active duty separation information (e.g., name, service number, date of birth, rank, sex, total amount of active service, branch of service, character of service, pay grade, assigned separation reason, service period, whether veteran was discharged with a disability, reenlisted, received a Purple Heart or other military decoration);
• payment information (e.g., veteran payee name, address, dollar amount of readjustment service pay, amount of disability or pension payments, number of nonpay days, any amount of indebtedness (accounts receivable) arising from title 38 U.S.C. benefits and which are owed to the VA);
• medical information (e.g., medical and dental treatment in the Armed Forces including type of service-connected disability, medical facilities, or medical or dental treatment by VA health care personnel or received from private hospitals and health care personnel relating to a claim for VA disability benefits or medical or dental treatment);
• personal information (e.g., marital status, name and address of dependents, occupation, amount of education of a veteran or a dependent, dependent’s relationship to veteran);
• education benefit information (e.g., information arising from utilization of training benefits such as a veteran trainee’s induction, reentrance or dismissal from a program or progress and attendance in an education or training program);
• applications for compensation, pension, education and vocational rehabilitation benefits and training which may contain identifying information, military service and active duty separation information, payment information, medical and dental information, personal and education benefit information relating to a veteran or beneficiary’s incarceration in a penal institution (e.g., name of incarcerated veteran or beneficiary, claims folder number, name and address of penal institution, date of commitment, type of offense, scheduled release date, veteran’s date of birth, beneficiary relationship to veteran and whether veteran or beneficiary is in a work release or half-way house program, on parole or has been released from incarceration). Etc.

PII Mapping of Components

DES VBA GSS consists of zero key components. Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by DES VBA GSS and the functions that collect it are mapped below.

PII Mapped to Components

<table>
<thead>
<tr>
<th>Components</th>
<th>Does this function collect or store PII? (Yes/No)</th>
<th>Type of PII</th>
<th>Reason for Collection of PII</th>
<th>Safeguards</th>
</tr>
</thead>
<tbody>
<tr>
<td>N/A</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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.

- Loan Guaranty Home, Condominium and Manufactured Home Loan Applicant Records
- Specially Adapted Housing Applicant Records, and Vendee Loan Applicant Records
- VA, Compensation, Pension, Education and Rehabilitation Records
- VA, Veterans and Beneficiaries Identification Records Location Subsystem
- VA. 36VA00 Veterans and Armed Forces Personnel United States Government Life Insurance Records
- VA. 46VA00 Veterans, Beneficiaries and Attorneys United States Government Insurance Award Records
- VA. 53VA00 Veterans Mortgage Life Insurance
- VA, Veterans and Beneficiaries Identification and Records Location (BIRLS)
- Compensation, Pension, Education, and Rehabilitation (covers BDN and Corporate databases)

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.

There are many VA forms used by veterans to apply for and/or make adjustments to pending benefits. All VBA benefit forms are located at https://www.va.gov/vaforms. The URL of the associated privacy statement is: https://www.va.gov/privacy. VBA forms can be downloaded from this site, filled in and printed to be delivered in paper form. All collected information is used to determine eligibility for benefits, process ratings and to provide payments via the Department of Treasury.

The VBA toll free number for veterans is 1-800-827-1000. Clients are referred to and transferred to the Regional Office of Jurisdiction, where they can provide a service representative with required information.

All collected information is used to determine eligibility for benefits, process ratings and to provide payments via the Department of Treasury. VBA employees may also contact a veteran directly to obtain clarifying information for a claim for benefits.

1.4 What is the purpose of the information being collected, used, disseminated, created, or maintained?
Include a statement of why the particular SPI is collected, maintained, used, or disseminated in the system is necessary to the program’s or agency’s mission. Merely stating the general purpose of the system without explaining why this particular type of information should be collected and stored is not an adequate response to this question.

If the system collects, uses, disseminates, or maintains publically available or commercial data, include a discussion of why commercial data is relevant and necessary to the system’s purpose.
This question is related to privacy control AP-2, Purpose Specification.

The VBA benefit systems accessed through the GSS, process entitlements for five mission areas: Compensation and Pension, Education, Vocational Rehabilitation and Employment, Loan Guaranty and Insurance. The primary services of the benefit systems entail the receipt, processing, tracking and disposition of veterans’ application for benefits and requests for assistance; and the general administration of legislated benefit programs. Information is collected to provide all entitled benefits in the most complete and effective manner. The information collected includes: Name, Address, Social Security Number, Family/Dependents, marital status, medical status, birth information, death information, service data; Reserve or Guard participation, retired pay or severance pay, hazardous agent exposure, branch of service, duty date, released date, type of discharge, separation reason, medical records, military clinical records, government health records, vocational rehabilitation and employment records, line of duty investigations to include police reports; incarceration at federal, state or local facility, fugitive felon status, and/or investigative reports for some accidents. The records may also contain additional veteran information such: Guardian information; court proceedings, field examinations, appointment and bonding of fiduciaries, and annual accounts. The benefit systems accessed through the GSS also contain veteran educational records such as: education program approval information, approved courses, effective dates, types of training, facility code, objective code and training type. Income verification is also used for veteran pension based decisions and entitlements. Most of the information provided above is kept in a central database not located at this facility but any of this information could be stored on the GSS at any given time during or after the processing of a VBA benefit.

1.5 How will the information be checked for accuracy?

Discuss whether and how 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?

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.

All data are matched against supporting claims documentation submitted by the veteran, widow, or dependent. Certain data such as SSN is verified with the Social Security Administration. Prior to any award or entitlement authorization(s) by the VBA, the veteran record is manually reviewed and data validated to ensure correct entitlement has been approved.

1.6 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

Generally, the authority to operate the Veterans Benefit Administration comes from 38 U.S. Code Chapter 77. Specific authority to operate the Des Moines Regional Office General Support System (GSS) is Title 10 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. This information is reflected in the VA SORN Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA, SORN 58VA21/22/28 (July 19, 2012).

1.7 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:** Sensitive Personal Information including personal contact information, service information and benefit information may be released to unauthorized individuals.

**Mitigation:**
- The Des Moines Regional Office adheres to information security requirements instituted by the VA Office of Information Technology (OIT).
- All employees with access to Veteran’s information are required to complete the VA Privacy and Information Security Awareness training and Rules of Behavior annually.
- The MS-Outlook default setting is configured to encrypt all email messages.
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.*

The record, or information contained in the record, may include identifying information (e.g., name, address, social security number); military service and active duty separation information (e.g., name, service number, date of birth, rank, sex, total amount of active service, branch of service, character of service, pay grade, assigned separation reason, service period, whether veteran was discharged with a disability, reenlisted, received a Purple Heart or other military decoration); payment information (e.g., veteran payee name, address, dollar amount of readjustment service pay, amount of disability or pension payments, number of nonpay days, any amount of indebtedness (accounts receivable) arising from title 38 U.S.C. benefits and which are owed to the VA); medical information (e.g., medical and dental treatment in the Armed Forces including type of service-connected disability, medical facilities, or medical or dental treatment by VA health care personnel or received from private hospitals and health care personnel relating to a claim for VA disability benefits or medical or dental treatment); personal information (e.g., marital status, name and address of dependents, occupation, amount of education of a veteran or a dependent, dependent’s relationship to veteran); education benefit information (e.g., information arising from utilization of training benefits such as a veteran trainee’s induction, reenrollment or dismissal from a program or progress and attendance in an education or training program); applications for compensation, pension, education and vocational rehabilitation benefits and training which may contain identifying information, military service and active duty separation information, payment information, medical and dental information, personal and education benefit information relating to a veteran or beneficiary’s incarceration in a penal institution (e.g., name of incarcerated veteran or beneficiary, claims folder number, name and address of penal institution, date of commitment, type of offense, scheduled release date, veteran’s date of birth, beneficiary relationship to veteran and whether veteran or beneficiary is in a work release or half-way house program, on parole or has been released from incarceration).

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

Letters to Veterans concerning the progress of their claim are generated periodically, as well as rating decisions and requests for additional information to substantiate the claim. These letters are generated electronically and printed on paper and mailed to the Veteran.

2.3 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.

- All employees with access to Veteran’s information are required to complete the VA Privacy and Information Security awareness training and rules of behavior annually.
- Disciplinary actions, depending on the severity of the offense, include counseling, loss of access, suspension and possibly termination.
- Individual users are given access to Veteran’s data through the issuance of a user ID and password, and by the use of a Personal Identity Verification (PIV) card. This ensures the identity of the user by requiring two-factor authentication. The user’s user ID limits the access to only the information required to enable the user to complete their job.

Section 3. Retention of Information

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

3.1 What information is retained?

Identify and list all information collected from question 1.1 that is retained by the system.

This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal

Name, Social Security Number, Date of Birth, Mailing Address, Zip Code, Phone Number, Email Address, Financial Account Information, Health Insurance Beneficiary Numbers, Previous Medical Records. Compensation, pension, and vocational rehabilitation claims 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. Official legal documents (e.g., birth certificates, marriage licenses) are returned to the claimant after copies are made for the claimant’s file. At the death of the veteran, these records are sent to the Federal Records Center (FRC), and maintained by the National Archives and Records Administration (NARA) in accordance with NARA policy. Some claims folders are electronically imaged; in which case, the electronic folder is maintained in the same manner as the claims folder. Once a file is electronically imaged and accepted by VBA, its paper contents (except for documents that are the official property of the Department of Defense, and official legal documents), are destroyed in accordance with Records Control Schedule VB–1 Part 1 Section XIII, as authorized by NARA. Documents that are the property of the Department of Defense are either stored at the RMC, or transferred to NARA and maintained in accordance with NARA policy. 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 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.

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.

This question is related to privacy control DM-2, Data Retention and Disposal.

Vocational rehabilitation claims 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. Official legal documents (e.g., birth certificates, marriage licenses) are returned to the claimant after copies are made for the claimant’s file. At the death of the veteran, these records are sent to the Federal Records Center (FRC), and maintained by the National Archives and Records Administration (NARA) in accordance with NARA policy. Some claims folders are electronically imaged; in which case, the electronic folder is maintained in the same manner as the claims folder. Once a file is electronically imaged and accepted by VBA, its paper contents (except for documents that are the official property of the Department of Defense, and official legal documents), are destroyed in accordance with Records Control Schedule VB–1 Part 1 Section XIII, as authorized by NARA. Documents that are the property of the Department of Defense are either stored at the RMC, or transferred to NARA and maintained in accordance with NARA policy.

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.
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 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.

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.

Records Control Schedule VB-1 Part 1, Section, XIII, Veterans Benefits Administration Records Management, Records Control Schedule VB–1, Part 1, Section VII

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.

Paper records are shredded on site by a shredding company and are accompanied by a certificate of destruction. Non-paper records maintained on magnetic media are destroyed by erasing the magnetic media using approved software to digitally overwrite the media. The media is then shipped to a contractor who destroys the magnetic media first by shredding the media and then by melting the shredded remains.

3.5 Does the system, where feasible, use techniques to minimize the risk to privacy of 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

Yes; where feasible to minimize the risk to privacy of using PII for research, testing, or training; no VA presentations or associated materials that may become publicly available shall contain PII or information exempt from release under the FOIA.
3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

Discuss the risks associated with the length of time data is retained and what steps, if any, are currently being taken to mitigate those identified risks.

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:
There is a risk that the information contained in the system will be retained for longer than is necessary to fulfill the VA mission.

Mitigation:
• Paper records are shredded monthly.
• All personnel with access to Veteran’s information are required to complete the VA Privacy and Information Security Awareness training and Rules of Behavior annually.
• The Des Moines Regional Office adheres to all information security requirements instituted by the VA Office of Information Technology (OIT).

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? What information is shared/received, and for what purpose? How is the information transmitted or disclosed?

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 information is 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.

<table>
<thead>
<tr>
<th>Program Office or IT System information is shared/received with</th>
<th>Reason why information is shared/received with the specified program or IT system</th>
<th>List the specific information types that are shared/received with the Program or IT system</th>
<th>Method of transmittal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Veterans Health Administration (VHA)</td>
<td>Determine eligibility for Veteran compensation</td>
<td>Name, Social Security Number, Date of Birth, Mailing Address, Zip Code, Phone Numbers, Email Address, Emergency Contact Information, Financial Account Information, Health Insurance Beneficiary Numbers, Current Medications, Previous Medical</td>
<td>Electronic transmission methods in accordance with VA policy. Paper records are shared with the VHA to conduct medical examinations to determine Veteran’s eligibility for compensation. The VHA accesses Veteran’s information in VBMS and VIS to verify eligibility.</td>
</tr>
</tbody>
</table>

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.

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

Follow the format below:

**Privacy Risk:** Privacy information may be released to unauthorized individuals.

**Mitigation:**
- All personnel with access to Veteran’s information are required to complete the VA Privacy and Information Security Awareness training and Rules of Behavior annually.
The Des Moines Regional Office adheres to all information security requirements instituted by the VA Office of Information Technology (OIT).

Information is shared in accordance with VA Handbook 6500.

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.

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 information is 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

<table>
<thead>
<tr>
<th>Program Office or IT System</th>
<th>Reason why information is shared/received with the specified program or IT system</th>
<th>List the specific information types that are shared/received with the Program or IT system</th>
<th>Legal authority, binding agreement, SORN routine use, etc that permit external sharing (can be more than one)</th>
<th>Method of transmission and measures in place to secure data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Iowa Department of Veteran Affairs</td>
<td>Assist Veterans with filing benefit claims.</td>
<td>Read only access to Covers, Share, VACOLS, Virtual VA, VBMS and MAP-D</td>
<td>SORN 58VA21/22/28 (July 19, 2012)</td>
<td>Electronic access to the local office GSS.</td>
</tr>
<tr>
<td>Disabled American Veterans</td>
<td>Assist Veterans with filing benefit claims.</td>
<td>Read only access to Covers, Share, VACOLS, Virtual VA, VBMS and MAP-D</td>
<td>SORN 58VA21/22/28 (July 19, 2012)</td>
<td>Electronic access to the local office GSS.</td>
</tr>
<tr>
<td>---------------------------</td>
<td>--------------------------------------------</td>
<td>-----------------------------------------------------------------</td>
<td>---------------------------------</td>
<td>---------------------------------</td>
</tr>
<tr>
<td>Military Order of the Purple Heart</td>
<td>Assist Veterans with filing benefit claims.</td>
<td>Read only access to Covers, Share, VACOLS, Virtual VA, VBMS and MAP-D</td>
<td>SORN 58VA21/22/28 (July 19, 2012)</td>
<td>Electronic access to the local office GSS.</td>
</tr>
<tr>
<td>Vietnam Veterans of America</td>
<td>Assist Veterans with filing benefit claims.</td>
<td>Read only access to Covers, Share, VACOLS, Virtual VA, VBMS and MAP-D</td>
<td>SORN 58VA21/22/28 (July 19, 2012)</td>
<td>Electronic access to the local office GSS.</td>
</tr>
<tr>
<td>American Legion</td>
<td>Assist Veterans with filing benefit claims.</td>
<td>Read only access to Covers, Share, VACOLS, Virtual VA, VBMS and MAP-D</td>
<td>SORN 58VA21/22/28 (July 19, 2012)</td>
<td>Electronic access to the local office GSS.</td>
</tr>
<tr>
<td>Veterans of Foreign Wars</td>
<td>Assist Veterans with filing benefit claims.</td>
<td>Read only access to Covers, Share, VACOLS, Virtual VA, VBMS and MAP-D</td>
<td>SORN 58VA21/22/28 (July 19, 2012)</td>
<td>Electronic access to the local office GSS.</td>
</tr>
</tbody>
</table>

If specific measures have been taken to meet the requirements of OMB Memoranda M-06-15 and M-06-16, note them here.

Co-located Veterans Service Organizations (VSOs) – Co-located Veterans Service Organizations at VBA regional offices have been given on-line read only access to Covers, Share, VACOLS, Virtual VA, VBMS and MAP-D. The co-located VSOs have access to veteran data securely through the GSS via Citrix Access Gateway (CAG). This access is authorized by VA regulations. The organization requests access and the standard VA logon and password security requirements that are applicable to VA employees are followed. Remote Veterans Service Organizations (VSOs) – Remote Veterans Service Organizations have been given on-line read only access to SHARE and COVERS. The remote VSOs access veteran data securely through Citrix Access Gateway (CAG). On-line access is real time and may be accessed by the County/State/National Service Organization at any time. This access is authorized by VA regulations. The County/State/National Service Organization requests on-line access for its representatives. The organization requests access and the standard VA logon and password security requirements that are applicable to VA employees are followed.

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:** Privacy information may be released to unauthorized individuals.

**Mitigation:**
- All personnel with access to Veteran’s information are required to complete the VA Privacy and Information Security Awareness training and Rules of Behavior annually.
- The Des Moines Regional Office adheres to all information security requirements instituted by the VA Office of Information Technology (OIT).
- Information is shared in accordance with VA Handbook 6500.
- All personnel accessing Veteran’s information must first have a successfully adjudicated fingerprint check. This fingerprint check is conducted by the Federal Bureau of Investigation (FBI) Justice Information and criminal history records. Individual users are given access to Veteran’s data through the issuance of a Personal Identity Verification (PIV) card. This ensures the identity of the user by requiring two-factor authentication (2FA).

### 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 following Written notice is on all VA forms: PRIVACY ACT INFORMATION: No allowance of compensation or pension may be granted unless this form is completed fully as required by law (38 U.S.C. 5101). The responses you submit are considered confidential (38 U.S.C. 5701). VA may disclose the information that you provide, including Social Security numbers, outside VA if the disclosure is authorized.
under the Privacy Act, including the routine uses identified in the VA system of records, 58VA21/22 Compensation, Pension, Education, and Rehabilitation Records - VA. The requested information is considered relevant and necessary to determine maximum benefits under the law. Information submitted is subject to verification through computer matching.

The Department of Veterans Affairs also provides notice by publishing the VA System of Record Notice (VA SORN) Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA, SORN 58VA21/22/28 (July 19, 2012), in the Federal Register and online. An online copy of the SORN can be found at: https://www.gpo.gov/fdsys/pkg/FR-2012-07-19/html/2012-17507.htm

This Privacy Impact Assessment (PIA) also serves as notice of the Des Moines Regional Office General Support System. As required by the eGovernment Act of 2002, Pub.Law 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.”

6.2 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

Benefits will not be provided without all required information being provided. No allowance of compensation or pension may be granted unless this form is completed fully as required by law (38 U.S.C. 5101). The requested information is considered relevant and necessary to determine maximum benefits under the law. Information submitted is subject to verification through computer matching.

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

Once information is provided to the VA, the records are used, as necessary, to ensure the administration of statutory benefits to all eligible Veterans, Service members, reservists, and their spouses, surviving spouses and dependents. As such, the Des Moines Regional Office does not provide individuals with the direct opportunity to consent to particular uses of information on the GSS. However, if an individual wishes to remove consent for a particular use of their information, they should contact the nearest VA regional office, a list of which can be found at https://benefits.va.gov/benefits/offices.asp

6.4 PRIVACY IMPACT ASSESSMENT: Notice

Describe the potential risks associated with potentially insufficient notice and what steps, if any, are currently being taken to mitigate those identified risks.
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:** Privacy information may be collected prior to providing the written notice.

**Mitigation:** The VA mitigates this risk by providing veterans and other beneficiaries with multiple forms of notice of information collection, retention, and processing. The 3 main forms of notice are discussed in detail in question 6.1 and include the Privacy Act statement, a System of Record Notice, and the publishing of this Privacy Impact Assessment.

**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.*

As directed in VA SORN Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA, SORN 58VA21/22/28 (July 19.2012), individuals seeking information regarding access to and contesting of VA records may write, call, or visit the nearest VA regional office. A list of regional VA offices may be found at: https://benefits.va.gov/benefits/offices.asp

**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.

The following procedure is from VA Handbook 6300.4:

(1) An individual may request amendment of a record pertaining to him or her contained in a specific VA system of records by mailing or delivering the request to the office concerned. The request must be in writing and must conform to the requirements in paragraph 3b(3) of this handbook. It must state the nature of the information in the record the individual believes to be inaccurate, irrelevant, untimely, or incomplete; why the record should be changed; and the amendment desired. The requester should be advised of the title and address of the VA official who can assist in preparing the request to amend the record if assistance is desired.

(2) Not later than 10 days, excluding Saturdays, Sundays, and legal public holidays, after the date of receipt of a request to amend a record, the VA official concerned will acknowledge in writing such receipt. If a determination has not been made, the acknowledgement will inform the individual when he or she may expect to be advised of action taken on the request. VA will complete a review of the request to amend or correct a record as soon as reasonably possible, normally within 30 days from receipt of the request (excluding Saturdays, Sundays, and legal public holidays).

(3) Where VA agrees with the individual's request to amend his or her record(s), the requirements of 5 U.S.C. 552a(d) will be followed. The record(s) will be corrected promptly and the individual will be advised promptly of the correction. Amendment consists of adding information to the record, altering information in the record, or deleting information in the record. Under the Privacy Act, if information is altered or deleted, the previous version must be obliterated and illegible after amendment. The amendment should be annotated "Amended, Privacy Act, (date), (signature and title of amending official)."

(4) If the record has previously been disclosed to any person or agency, and an accounting of the disclosure was made, prior recipients of the record will be informed of the correction. FL 70-19, Notification to Other Person or Agency of Amendment to a Record, may be used.

(5) If it is determined not to grant all or any portion of the request to amend a record, the official will promptly notify the individual in writing. The individual will be advised of his or her right to file a concise statement of reasons for disagreeing with the refusal to amend. The notice will specify the reason(s) for denying the request, identify the VA regulations or statutes upon which the denial is based, and advise that the denial may be appealed in writing to the General Counsel (024), Department of Veterans Affairs, 810 Vermont Avenue, NW, Washington, DC 20420. FL 70-20, Notification of Initial Refusal to Amend a Record Under the Privacy Act, may be used for this purpose.

(6) The determination on an appeal will be made not later than 30 days, excluding Saturdays, Sundays, and legal public holidays, from the date the individual's letter of appeal is received unless the Secretary or Deputy Secretary, for good cause shown, extends such 30-day period. If the 30-day period is so extended, the individual will be notified promptly of the reasons for the extension and the date on which a final determination may be expected. The final determination in such appeals will be made by the General Counsel or Deputy General Counsel.

(7) If the General Counsel or Deputy General Counsel finds that the adverse determination should be reversed, he or she will notify the VA office or station of the remedial action to be taken. The VA office or station will promptly carry out that action. The General Counsel or Deputy General Counsel will promptly notify the individual in writing of the corrective action. The field station or Central
Office organization that provided the initial decision will inform previous recipients of the record that a correction has been made.

(8) If the General Counsel or Deputy General Counsel determines that the adverse determination will not be reversed, the individual will be notified promptly in writing of that determination, the reasons therefor, and of his or her right to seek judicial review of the decision pursuant to section 3 of the Privacy Act (5 U.S.C. 552a(g)).

(9) If the adverse determination is sustained by the General Counsel or Deputy General Counsel, the individual will also be advised promptly of his or her right to file a concise statement of reasons for disagreeing with the refusal to amend. The statement may contain information that the individual believes should be substituted.

(10) When an individual file a statement disagreeing with VA's decision not to amend a record, the record will be clearly annotated so that the fact that the record is disputed is apparent to anyone who may subsequently access, use, or disclose it. When the disputed record is disclosed to persons or other agencies, the fact of the dispute will be clearly noted. Copies of the statement of disagreement will be provided, and, when appropriate, copies of a concise statement of VA's reasons for not making the amendment(s) requested will also be provided.

(11) A decision by either the General Counsel or Deputy General Counsel pursuant to paragraph 3f(7) of this handbook is final. It is subject to judicial review in the district court of the United States in which the complainant resides, or has his or her principal place of business, or in which the VA records are located, or in the District of Columbia.

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.

Veterans and other beneficiaries are notified of the procedures for correcting their records at the VA through VA SORN Compensation, Pension, Education and Employment Records-VA, SORN 58VA21/22/28(July 19, 2012), which states:

Records Access Procedures:
Individuals seeking information regarding access to and contesting of VA records may write, call or visit the nearest VA regional office. Address locations are listed in VA Appendix 1. The list of VA regional offices referenced in the SORN can also be found at: https://benefits.va.gov/benefits/offices.asp

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 stored in the Des Moines Regional Office GSS, however, veterans and other beneficiaries may contact their local VA regional office to learn how to access their VA records and correct, if necessary, the records used by the GSS.

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 that members of the public will not know the relevant procedures for gaining access to, correcting or contesting their information.

Mitigation: This privacy risk is mitigated by information provided in VA SORN Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA, SORN 58VA21/22/28(July 19, 2012). This states that individuals should contact their local VA regional office for additional information about accessing and contesting their records at the VA.

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.

- Individuals are subject to a background investigation before given access to Veteran’s information.
- All personnel with access to Veteran’s information are required to complete the VA Privacy and Information Security Awareness training and Rules of Behavior annually.

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 or a Non-Disclosure Agreement (NDA) been developed for contractors who work on the system?

If so, how frequently are contracts reviewed and by whom? Describe the necessity of the access provided to contractors to the system and whether clearance is required. If Privacy Roles and Responsibilities have been established to restrict certain users to different access levels, please describe the roles and associated access levels. Explain the need for VA contractors to have access to the PII.

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

Contractors will have access to the system after the promulgation of a background investigation and completing the VA Privacy and Information Security Awareness training and Rules of Behavior initially and annually thereafter.

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.

VA requires Privacy and Information Security Awareness training be completed on an annual basis. The Talent Management System offers the following applicable privacy courses:

- VA 10176: Privacy and Information Security Awareness and Rules of Behavior
- VA 10203: Privacy and HIPPA Training
- VA 3812493: Annual Government Ethics

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

If so, provide the date the Authority to Operate (ATO) was granted. Please note that all systems containing SPI are categorized at a minimum level of “moderate” under Federal Information Processing Standards Publication 199.

The Des Moines Regional Office GSS is categorized as Medium in accordance with Federal Information Processing Standards Publication (FIPS) 199. The Des Moines Regional Office GSS is currently operating under an ATO dated September 19, 2016.
## Section 9. References

### Summary of Privacy Controls by Family

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

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

_________________________________________
Privacy Officer, Stacey A. Lampe

_________________________________________
Information Security Officer, Terrence A. Rausch

_________________________________________
System Owner, Mary Barley
APPENDIX A-6.1

Notice of Privacy Practices

Effective Date:

Please provide a copy of the notice below (A notice may include a posted privacy policy, a Privacy Act notice on forms).

Privacy Act Notice from VA form 21-4138:

The VA will not disclose information collected on this form to any source other than what has been authorized under the Privacy Act of 1974 or Title 38, Code of Federal Regulations 1.576 for routine uses (i.e., civil or criminal law enforcement, congressional communications, epidemiological or research studies, the collection of money owed to the United States, litigation in which the United States is a party or has an interest, the administration of VA Programs and delivery of VA benefits, verification of identity and status, and personnel administration) as identified in the VA system of records, 58VA21/22/28, Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records - VA, published in the Federal Register. Your obligation to respond is required to obtain or retain benefits. VA uses your SSN to identify your claim file. Providing your SSN will help ensure that your records are properly associated with your claim file. Giving us your SSN account information is voluntary. Refusal to provide your SSN by itself will not result in the denial of benefits. The VA will not deny an individual benefits for refusing to provide his or her SSN unless the disclosure of the SSN is required by Federal Statute of law in effect prior to January 1, 1975, and still in effect. The requested information is considered relevant and necessary to determine maximum benefits under the law. The responses you submit are considered confidential (38 U.S.C. 5701). Information submitted is subject to verification through computer matching programs with other agencies.

PRIVACY ACT INFORMATION: The VA will not disclose information collected on this form to any source other than what has been authorized under the Privacy Act of 1974 or Title 38, Code of Federal Regulations 1.576 for routine uses (i.e., civil or criminal law enforcement, congressional communications, epidemiological or research studies, the collection of money owed to the United States, litigation in which the United States is a party or has an interest, the administration of VA Programs and delivery of VA benefits, verification of identity and status, and personnel administration) as identified in the VA system of records, 58VA21/22/28, Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records - VA, published in the Federal Register. Your obligation to respond is required to obtain or retain benefits. VA uses your SSN to identify your claim file. Providing your SSN will help ensure that your records are properly associated with your claim file. Giving us your SSN account information is voluntary. Refusal to provide your SSN by itself will not result in the denial of benefits. The VA will not deny an individual benefits for refusing to provide his or her SSN unless the disclosure of the SSN is required by Federal Statute of law in effect prior to January 1, 1975, and still in effect. The requested information is considered relevant and necessary to determine maximum benefits under the law. The responses you submit are considered confidential (38 U.S.C. 5701). Information submitted is subject to verification through computer matching programs with other agencies.

RESPONDENT BURDEN: We need this information to obtain evidence in support of your claim for benefits (38 U.S.C. 501(a) and (b)). Title 38, United States Code, allows us to use for this information. We estimate that you will need an average of 15 minutes to review the instructions, find the information, and complete this form. VA cannot conduct or sponsor a collection of information unless a valid OMB control number is displayed. You are not required to respond to a collection of information if you choose not to participate. Valid OMB control numbers can be located on the OMB Internet Page at www.whitehouse.gov/omb. If desired, you may call 1-800-827-1000 to get information on where to send comments or suggestions about this form.

VA FORM 21-4138, DEC 2017