Privacy Impact Assessment for the VA IT System called:

Common Security Service (CSS)

Benefits and Memorials Services
Veterans Benefits Administration (VBA)

Date PIA submitted for review:

08-15-2022

System Contacts:

System Contacts

Role	Name	E-mail	Phone Number
Privacy Officer	Jean-Claude Wicks	Jean-Claude.Wicks@va.gov	202-502-0084
Information System Security Officer (ISSO)	Tamer Ahmed	Tamer.Ahmed@va.gov	202-461-9306
Information System Owner	Lindsay Tucker	Lindsay.Tucker@va.gov	202-461-6126

Abstract

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

Common Security Services (CSS) is the underlying security application providing access and authentication services to in-house developed VBA client-server and Web-Logic applications. CSS controls who, and to what extent, VA employees and Veteran Service Officers (VSOs), can access, establish, and develop Veterans' claims. Data extracted by the Benefits Delivery Network, (BDN), Veteran Service Organization (VSO), State Approving Agency (SAA), and VBA is used to verify access rights and permission levels of the User requesting the 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*
- *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.*
- *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.*
- *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?*

- Common Security Services (CSS) resides on the VBA Corporate Database (CRP), that is hosted by the Austin Information Technology Center (AITC). CSS is owned by the Veterans Benefits Administration (VBA) Office of Business Process Integration (OBPI).
- Common Security Services (CSS) is the underlying security application providing access and authentication services to in-house developed VBA client-server and Web-Logic applications. CSS controls who, and to what extent, VA employees and Veteran Service Officers (VSOs), can access

data within the VBA Corporate Database (CRP) for the purpose of accessing, establishing, and developing Veterans' claims.

- CSS is a suite of security applications that consist of the following: Common Security Employee Manager (CSEM), Common Security Application Manager (CSAM), Common Security User Manager (CSUM), Authentication DLL, and Station Switch. These components provide access control and privacy protection to systems that use the VBA corporate environment. The VBA Corporate Database (CRP) maintains all PII. No PII is stored within CSS. CSS controls who, and to what extent, VA employees and Veteran Service Officers (VSOs), can access, establish, and develop veterans' claims. Data extracted by the Benefits Delivery Network, (BDN), Veteran Service Organization (VSO), State Approving Agency (SAA), and VBA is used to verify access rights and permission levels of the User requesting the information.
- CSS falls within the BAM portfolio – BIA.
- CSS was adopted by VBA to be the single point of entry for the VBA's mission critical benefit payment systems residing in the VBA corporate environment. Relying on one access control software mitigates security risks, reduces redundancy, and eliminates incompatibilities when trying to apply security policies to multiple security access control devices. CSS implements security access policy in a single solution.
- Data transmitted within the VBA Corporate Environment is encrypted. CSS does not store any PII, itself. All PII is stored in the VBA Corporate Database which is not part of the CSS accreditation boundary.
- CSS provides approximately 50,000 active employees access to VBA applications.
- System of Record Notice (SORN) ''VA Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records—VA'' (58VA21/22/28) states the legal authority to maintain the system 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.
- Completion of this PIA will not result in circumstances that require changes to business process.
- Completion of this PIA is not anticipated to result in technology changes.
- Completion of this PIA is not anticipated to result changes to the SORN.
- The system does not utilize 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)

CSS User Identification, Benefit Delivery Network (BDN) Employee Identifier Number (EIN), VA Claim Number.

Access control can also be based on Social Security Number (SSN) of the Veteran. CSS users are required to complete an electronic VA Form 20- 8824E, CSS User Access Request Form. This form is used by the CSS Business Owner and ISO to communicate the business need and justification for access to the VBA Corporate systems. This form collects the following information:
Duty Station, Veteran File number, Job Title, GS Level, Job Code, Organization/Division, User's Supervisor, Supervisor's Job Title, Supervisor's Phone Number, Local Area Network ID, Sensitive Access Level, Super Diagnostic Code Description, Veteran Service Organization Codes, Contractor/Work study End Date, Action Requested (new access, delete, update, delete SMGW registration), Environment Requested (Development, Certification, Pre-Production, Integrated, Academy.

PII Mapping of Components

Common Security Services consists of zero (0) key components (databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by Common Security Services and the reasons for the collection of the PII are in the table below.

Common Security Services does NOT contain a database.

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
N/A – CSS has no Databases					

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.

Sources of information are from the VA Benefit Delivery Network (BDN), Veteran Service Organization (VSO), Veteran Benefits Administration (VBA), State Approving Officials (SAA), Veterans and Individuals with power of attorney that request access to one of the VBA applications to support a veteran.

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.

VA FORM 20-0344 is submitted annually by VBA employees. It lists the employee's relatives who are veterans and lists the SSN and/or file number of the relatives. The OMB Control number for VA form 20-0344 is 2900-0654. The information is transmitted through an encrypted link to the VBA Corporate Database.

CSEM and CSAM use Simple Object Access Protocol – (SOAP) for internal electronic transmission between the VA Benefit Delivery Network (BDN), Veteran Service Organization (VSO), and the Veteran Benefits Administration (VBA) systems.

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.

The intended use of information collected by CSS is to control access to Veteran information as authorized by the Information System Owner (ISO). CSS users are required to have a completed CSS User Access Request Form VA FORM 0344 on file. CSS forces security checks on all VBA applications. A user is not able to able to add or delete information stored in the VBA Corporate Database (CRP) without being authenticated through CSS. There is no actual data to check within CSS as all data is housed within CRP.

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

Title 10 United States Code (U.S.C.) chapters 106a, 510, 1606 and 1607 and Title 38, U.S.C., section 501(a) and Chapters 11, 13, 15, 18, 23, 30, 31, 32, 33, 34, 35, 36, 39, 51, 53, and 55.

VA SORN Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA, SORN 58VA21/22/28(November 8, 2021) the following: Records Control Schedule VB-1 Part 1, Section, XIII, Veterans Benefits Administration Records Management, Records Control Schedule VB–1, Part 1, Section VII apply.

The official system of records notice (SORN) for "Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA" (58VA21/22/28) can be found on-line at http://www.oprm.va.gov/privacy/systems_of_records.aspx.

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

Mitigation: All personnel with access to the VA network and Veteran's information are required to complete the VA Privacy, Information Security Awareness training and Rules of Behavior annually. In addition to training, a security check is used to verify whether the CSS application user has the access level needed to view the Veteran's file. If the user has a sufficient level of

access to view the record, the record is provided to the user. If not, access is denied and the attempt is logged, and will show up on a report provided to the Information Security Officers (ISOs).

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 following information is collected by CSS. CSS User Identification, Benefit Delivery Network (BDN) Employee Identifier Number (EIN), VA Claim Number.

Intended use of information is to control access to veteran information as authorized by the system Information Owner and ISO. Data extracted by the BDN, VSO, SAA and VBA is used to verify access rights and permission levels of the User requesting the information.

Veteran Benefits Administration (VBA): VA Claim Number: Is used to control access to veteran files by searching for VA Claim Number for Corporate applications. When a veteran record is retrieved from
Corporate or BDN by an application, before the information is presented to the user requesting the file,
CSS security checks to see if the VA Claim Number is found in a special file called a "sensitive record" file. CSS maintains the sensitive record file as a means of further restricting access to certain veteran records that the Information Owner has designated as requiring restricted access. The sensitive record file is stored on the VBA Corporate Database and is part of its accreditation boundary.

If a veteran's file is found that matches the user's inquiry, CSS will verify the user's security record to determine if the employee has sufficient credentials to access the file. If the employee attempting to access a
VA Claim Number listed in the Sensitive Record file lacks sufficient credentials to view the file, CSS blocks access to the file, and sends a message to the user to contact their supervisor.

Access control is based on SSN for VSOs and SAAs. All users are required to complete a CSS User Access Request form (VA Form 20-8824E). Utilization of this form is how the business owner communicates the business need and justification for access to VBA Corporate systems. The ISO audits the approval to ensure the supervisor and second-line supervisor followed procedures and everything is in order.

Reasons for the information collected in VA Form 20- 8824E 8824Eis as follows:

- Name – To identify that person in case of an incident
- Duty Station – Specifies what station the user will login to when accessing VBA Applications
- Social Security Number- Unique identifier collected to verify whether or not the employee is a veteran
- Veteran File number – This is only collected if the employee, or external entity, is a veteran
- Job Title – Specifies what type of work the employee will be doing within the VBA System
- GS Level – This is collected since certain features in other applications have a requirement that an employee must be above a certain grade level to perform cert functions within that application. This is used to determine whether or not the user is allowed to perform that function.
- Job Code – This identifies the office of the User, but is not stored in CSS and is mainly used by HR
- Organization/Division – Used to gain access to supervisor information so that CSEM Electronic access requests can be approved properly by the employee's supervisor
- Duty Phone – Contact for the employee
- Duty Email Address – This is required to help match the Active Directory User ID with the CSS User ID using the employee's e-mail address.
- Cell Phone/Pager – Contact the employee, as needed
- User's Supervisor – Supervisor is required to place the employee in the correct division so the supervisor can approve all electronic requests for access through CSEM
- Supervisor's Job Title – Verifies the Supervisor's job title
- Supervisor's Phone Number – Contact for the Supervisor
- Local Area Network ID – This is the unique User ID given to the employee through Active Directory and is required for access to VBA Applications
- Employee ID Number- This is the corresponding BDN EIN number required if the user is given access to applications that interact with the BDN so that security violations can be recorded and moved into VBA Corporate Database for reporting purposes for the ISO community
- Sensitive Access Level – This is the record level the user is allowed to access within the sensitive file for those veterans who have their record sensitized
- Super Diagnostic Code Description – This is an indicator for other applications to suppress certain diagnostic codes (including HIV/AIDS and Sickle Cell Anemia)
- Veteran Service Organization Codes – If the employee is a VSO this is where the Power of Attorney codes provide the User access to the VBA system(s) based on their access level and whether they have Power of Attorney over the record.
- Contractor/Work study End Date – If the employee has an end date this must be recorded. When the end date is reached the user's record will be automatically locked (in case the contract is not renewed). If the contract is renewed, the ISO or Security Officer will update the Contract End Date so the user can resume their access.
- Action Requested (new access, delete, update, delete SMGW registration) – Indicates whether this is a request for new access, updated access or deletion of the access to the deletion of the SMGW registration
- Environment Requested (Production, Development, Certification, Pre-Production, Integrated, Academy) – Specifies the environment to which the User will be allowed access

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

CSS itself is a tool used to analyze data. CSS ensures each user accessing a Veteran's record within a VBA application (that resides in the VBA Corporate Database and is pushed to each user at a VA Regional Office) has the sufficient level of access needed to view that record. If the user does not have the sufficient level of access required to view the record, access is denied, and the attempt is logged on a report that is provided to the Information Security Officers (ISOs). The ISOs then review the report and ask for justification for attempted access to the record.

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?

- Benefits Enterprise Platform (BEP) and VBA Corporate Database (CRP), under the accreditation boundary of VBA Corporate Infrastructure (CRP-BEP), provide protection for data in transit and at rest. CSS does not have a database in its accreditation boundary.

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

- Only privileged users are allowed access to CSS and only certain roles with a need to know can view the entire Social Security Number.

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

- .CSS does not maintain any PII. The PII is transmitted via BEP webservices and stored within the VBA Corporate Database (CRP) which is accredited under VBA Corporate Infrastructure (CRP-BEP).

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.

The controls in place, ensuring that information is handled properly are as follows: The minimum security requirements for CSS's moderate impact system cover 17 security-related areas with regard to protecting the confidentiality, integrity, and availability of VA information systems and the information processed, stored, and transmitted by those systems. The security-related areas include access control; awareness and training; audit and accountability; certification, accreditation, and security assessments; configuration management; contingency planning; identification and authentication; incident response; maintenance; media protection; physical and environmental protection; planning; personnel security; risk assessment; systems and services acquisition; system and communications protection; and system and information integrity. All security controls in the respective moderate impact security control baseline are employed unless specific exceptions have been allowed based on the tailoring guidance provided in NIST Special Publication 800-53 and specific VA directives.
Users are trained how to handle sensitive information by taking VA Privacy and Security Awareness Rules of Behavior training (mandatory for all personnel with access to sensitive information or access to VA network). After completing the course, users read and attest they understand the VA Rules of Behavior. Users must take a refresher course, 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 using 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

CSS only uses the SSN and VBA file number. External CSS users gain access to the VA Network by filling out VA Form 20- 8824E(or CSEM) where the following user information is collected and stored in the VBA Corporate Database, not in CSS itself:

Name, Duty Station, Social Security Number, Veteran File number, Job Title, GS Level, Job Code, Organization/Division, Duty Phone, Duty Email Address, Cell Phone/Pager, User's Supervisor, Supervisor's Job Title, Supervisor's Phone Number, Local Area Network ID, Employee ID Number, Sensitive Access Level, Super Diagnostic Code Description, Veteran Service Organization Codes, Contractor/Work study End Date, Action Requested (new access, delete, update, delete SMGW registration), Environment Requested (Development, Certification, Pre-Production, Integrated, Academy)

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.

Per VA SORN 58VA21/22/28:
Records are maintained at VA regional offices, VA centers, the VA Records Management Center (RMC), St. Louis, Missouri, the Data Processing Center at Hines, Illinois, the Corporate Franchise Data Center in Austin, Texas, the Information Technology Center at Philadelphia, PA., and IBM GTS Cloud Transformation Services in Culpepper, VA. Active records are generally maintained by the regional office having jurisdiction over the domicile of the claimant. Active educational assistance records are generally maintained at the regional processing office having

jurisdiction over the educational institution, training establishment, or other entity where the claimant pursues or intends to pursue training. The automated individual employee productivity records are temporarily maintained at the VA data processing facility serving the office in which the employee is located. The paper record is maintained at the VA regional office having jurisdiction over the employee who processed the claim. Records provided to the Department of Housing and Urban Development (HUD) for inclusion on its Credit Alert Interactive Voice Response System (CAIVRS) are located at a data processing center under contract to HUD at Lanham, Maryland. Address locations of VA facilities are listed in the VA Appendix I and are also listed at http://www2.va.gov/directory/guide/home.asp?isFlash=1 .

CSS deals only with electronic records that are stored and maintained in the VBA Corporate Database which is not part of the CSS accreditation boundary.

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 recording retention schedule may be found via the SORN associated with the system (VA SORN Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA, SORN 58VA21/22/28(November 8, 2021) which states: Records Control Schedule VB-1 Part 1, Section, XIII, Veterans Benefits Administration Records Management, Records Control Schedule VB–1, Part 1, Section VII apply.

The official system of records notice (SORN) for "Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA" (58VA21/22/28) can be found on-line at https://www.oprm.va.gov/privacy/systems_of_records.aspx

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

All CSS data is stored in the VBA Corporate Database and is not part of the CSS accreditation boundary; therefore, the elimination of SPI is not handled by CSS.

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

All users of CSEM and CSUM that require access to data containing PII must go through an approval process that requires signatures from Supervisors/CORs and Directors. Other users not requiring access to PII data can use CSEM and CSUM in test environments which only contains mock data.

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; however, this risk would fall upon the accreditation boundary of the VBA Corporate Database since the PII is maintained within it, not CSS itself. The Privacy Risk and Mitigation noted in the CRP Privacy Impact Assessment dated 05-29-2015 states:
As described herein, support systems retain information until that work in progress is completed and data is committed to master systems and records. The master systems retain data on a permanent basis (beyond the actual death of the veteran). If a master system is to be deactivated, critical information is migrated to the new system and the old system along with associated data is archived according to the application disposition worksheet. As such, SPI, PII or PHI may be held for long after the original record was required to be disposed. This extension of retention periods increases the risk that SPI may be breached or otherwise put at risk.

Mitigation: Redaction of some information is required by law and protects the privacy interest of any individual who may have SPI, PII or PHI which may appear in the data and files collected.

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.

CSS is the underlying security application providing access control to in-house developed VBA client-server and Web-Logic applications. It authenticates users to VBA applications and Veteran data in the VBA Corporate database, and it allows the Regional Offices to control access to VBA applications, roles, functions, and data.
The application provides security services to applications throughout VBA. When a user searches for a Veteran record in an application that uses the VBA production environment the VBA corporate database, (e.g., VETSNET, Virtual VA, WINRS), or Benefits Delivery Network (BDN) or IBS the request goes through CSS written code that checks to validate the user is allowed access to the record and whether that access is limited to read-only or updates are allowed. No data is provided to CSS or any end users during this check; however, if the check meets certain criteria, the access is logged in tables in VBA Corporate database (no PII is stored in the process, merely pointers to the record of the person requesting access and the record that they attempted to access).

CSS maintains the sensitive record file (a table within the VBA Corporate Database), and is part of that systems ATO, as a means of further restricting access to certain veteran records that the Information Owner has designated as requiring restricted access. If a veteran file is found that matches the user's inquiry, CSS verifies the user's security record to determine if the employee has sufficient credentials to access the file. If the employee attempting to access a VA Claim Number listed in the Sensitive Record file lacks sufficient credentials to view the file, CSS blocks access to the file, and sends a message to the user to contact their supervisor, as well as logging the attempt to access the file in security tables located in VBA corporate.

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***
VBA Corporate Infrastructure (VBA Corporate Database)	When a VBA application user tries to access a Veteran record that is stored in the VBA Corporate database, a comparison is made between the Veteran's claim number and the information stored in an Oracle table (referred to as a sensitive file) which is also maintained in the VBA Corporate Database. The comparison verifies whether the application user has the access level needed to view the Veteran's file. If the user has a sufficient level of access to view the record, the record is provided to the application. If	VA Claim Number, Name, Duty Station, Social Security Number, Veteran File number, Job Title, GS Level, Job Code, Organization/Division, Duty Phone, Duty Email Address, Cell Phone/Pager, User's Supervisor, Supervisor's Job Title, Supervisor's Phone Number, Local Area Network ID, Employee ID Number, Sensitive Access Level, Super Diagnostic Code Description, Veteran Service Organization Codes, Contractor/Workstudy End Date, Action Requested (new access, delete, update, delete SMGW registration), Environment Requested (Development, Certification, Pre-Production, Integrated, Academy	Encrypted Tuxedo connection

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*
	not, the attempt is logged, and will show up on a report provided to the station Information Security Officers (ISOs). The CSS applications (CSEM/CSUM) are used by ISOs to set the sensitive record level of the Veteran's records and the access level of the individuals doing the look up, but all of the data, and the code that actually does the comparison is done within the VBA Corporate Database.		
Veterans Benefits Administration / Benefits Delivery Network (BDN)	The CSS applications (CSEM/CSUM) are used by ISOs to set the sensitive record level of the Veteran's records and the access level of the individuals doing the look up, but all of the data, and the code that actually does the comparison is part of VBA Corporate Applications (CRP).	VA Claim Number Name, Duty Station, Social Security Number, Veteran File number, Job Title, GS Level, Job Code, Organization/Division, Duty Phone, Duty Email Address, Cell Phone/Pager, User's Supervisor, Supervisor's Job Title, Supervisor's Phone Number, Local Area Network ID, Employee ID Number, Sensitive Access Level, Super Diagnostic Code Description, Veteran Service Organization Codes, Contractor/Workstudy End Date, Action Requested (new	Encrypted Tuxedo connection

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*
		access, delete, update, delete SMGW registration), Environment Requested (Development, Certification, Pre-Production, Integrated, Academy	

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:

Sharing of protected Veteran data is necessary to support VA benefits processing/ensure eligible Veterans receive the VA benefits to which they are entitled; however, sharing of any information carries with it a risk of unauthorized disclosure.

Mitigation: The risk of improperly disclosing protected Veteran data to an unauthorized internal VA entity and/or VA personnel is mitigated by limiting access only those VA entities and personnel with approved access and clear business purpose/need to know. Additionally, consent for use of PII data is signaled by the completion of benefits forms by the Veteran. The principle of need to know is strictly adhered to. 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.

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***
Veterans Service Organizations (VSOs)	Veterans request assistance of VSO and State Approving Agency (SAA) Officials using VA Form 21-22 and solicit help from VA-	The Veteran submits VA Form 21-22 through SHARE (another VBA application) claiming the need for the Power of Attorney or VSO to be granted permission to access the veteran's data on their behalf. Once VA form 21-22 has been submitted, the Power of Attorney or VSO submits an Access Request form	VA Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records—VA'' (58VA21/22/28) states the legal authority	Encrypted Tuxedo Connection

	accredited attorney or claims agent (via VA Form 21-22a) as their power of attorney regarding a claim. These limited powers of attorney authorize the designated organization or individual to act on behalf of the claimant in the preparation, presentation, and prosecution of a claim. VSO-SAA Officials, Attorneys and Claim Agents share their own data when applying for an internal VA account (using VA Form 20-8824E 8824Eaccess VBA systems. VA Form 20- 8824E 8824Eis a User Access Request form that is used for the Business	(VA Form 20- 8824E8824E) through CSS to gain access to the veteran's data. Once the Power of Attorney or VSO have a valid 8824E form on file, CSS will allow the VSO or Power of attorney access to the veterans data contained in the VBA applications that reside within the VBA Corporate Database. The following information is obtained on form 8824E: Name, Duty Station, Social Security Number, Veteran File number, Job Title, GS Level, Job Code, Organization/Division, Duty Phone, Duty Email Address, Cell Phone/Pager, User's Supervisor, Supervisor's Job Title, Supervisor's Phone Number, Local Area Network ID, Employee ID Number, Sensitive Access Level, Super Diagnostic Code Description, Veteran Service Organization Codes, Contractor/Workstudy End Date, Action Requested (new access, delete, update, delete SMGW registration), Environment Requested (Development, Certification, Pre-Production, Integrated, Academy)	to maintain the system 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	

	Owner and CSS ISO to communicate the business need and justification for the VSOs and SAAs to be granted access to one of the VBA Corporate Systems.			
State Approving Agencies (SAA)	Veterans request assistance of VSO and State Approving Agency (SAA) Officials using VA Form 21-22 and solicit help from VA-accredited attorney or claims agent (via VA Form 21-22a) as their power of attorney regarding a claim. These limited powers of attorney authorize the designated organization or individual to act on behalf of the claimant in the preparation, presentation,	The Veteran submits VA Form 21-22 through SHARE (another VBA application) claiming the need for the Power of Attorney or VSO to be granted permission to access the veteran's data on their behalf. Once VA form 21-22 has been submitted, the Power of Attorney or VSO submits an Access Request form (VA Form 20- 8824E8824E) through CSS to gain access to the veteran's data. Once the Power of Attorney or VSO have a valid 8824E form on file, CSS will allow the VSO or Power of attorney access to the veterans data contained in the VBA applications that reside within the VBA Corporate Database. The following information is obtained on form 8824E: Name, Duty Station, Social Security Number, Veteran File number, Job Title, GS Level, Job Code, Organization/Division, Duty Phone, Duty Email Address, Cell Phone/Pager, User's Supervisor, Supervisor's Job Title, Supervisor's Phone	VA Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records—VA'' (58VA21/22/28) states the legal authority to maintain the system 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	Encrypted Tuxedo Connection

	and prosecution of a claim. VSO-SAA Officials, Attorneys and Claim Agents share their own data when applying for an internal VA account (using VA Form 20-8824E 8824Eto access VBA systems.	Number, Local Area Network ID, Employee ID Number, Sensitive Access Level, Super Diagnostic Code Description, Veteran Service Organization Codes, Contractor/Workstudy End Date, Action Requested (new access, delete, update, delete SMGW registration), Environment Requested (Development, Certification, Pre-Production, Integrated, Academy)		
VA Accredited Attorney or Claims Agent	Veterans request assistance of VSO and State Approving Agency (SAA) Officials using VA Form 21-22 and solicit help from VA-accredited attorney or claims agent (via VA Form 21-22a) as their power of attorney regarding a claim. These limited powers of attorney authorize the designated organization or individual	The Veteran submits VA Form 21-22 through SHARE (another VBA application) claiming the need for the Power of Attorney or VSO to be granted permission to access the veteran's data on their behalf. Once VA form 21-22 has been submitted, the Power of Attorney or VSO submits an Access Request form (VA Form 20- 8824E8824E) through CSS to gain access to the veteran's data. Once the Power of Attorney or VSO have a valid 8824E form on file, CSS will allow the VSO or Power of attorney access to the veterans data contained in the VBA applications that reside within the VBA Corporate Database. The following information is obtained on form 8824E: Name, Duty Station, Social Security Number, Veteran File number, Job Title, GS Level,	VA Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records—VA'' (58VA21/22/28) states the legal authority to maintain the system 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	Encrypted Tuxedo Connection

	to act on behalf of the claimant in the preparation, presentation, and prosecution of a claim. VSO-SAA Officials, Attorneys and Claim Agents share their own data when applying for an internal VA account (using VA FORM VA Form 20-8824E8824E) to access VBA systems. VA Form 20- 8824E 8824Eis a User Access Request form that is used for the Business Owner and CSS ISO to communicate the business need and justification for the VSOs and SAAs to be granted access to one of the VBA	Job Code, Organization/Division, Duty Phone, Duty Email Address, Cell Phone/Pager, User's Supervisor, Supervisor's Job Title, Supervisor's Phone Number, Local Area Network ID, Employee ID Number, Sensitive Access Level, Super Diagnostic Code Description, Veteran Service Organization Codes, Contractor/Workstudy End Date, Action Requested (new access, delete, update, delete SMGW registration), Environment Requested (Development, Certification, Pre-Production, Integrated, Academy)		

	Corporate Systems.			

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: The VA cannot control what the VSOs, SAAs, and VA accredited attorneys or claims agents do with the data they view, after they view it; therefore it could potentially be shared with entities and individuals without proper permissions to access the data; however, that risk would fall on the application through which the user was accessing that is stored within the VBA Corporate Database, not on CSS, itself. CSS does not store or maintain PII.

Mitigation: QRadar produces audit logs of the VBA Corporate Database which is where all PII for CSS is stored. ISOs also review records in the sensitive record file, at least every 3 years. All external entities access the data from an internal VA account, behind the VA firewall. Privacy is further secured by storing all data on encrypted local servers behind firewalls and external users are vetted and trained in the same exact manner as VA employees.

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.

Privacy notice is provided via the Internet site (http://www.va.gov/privacy/) and the SORN 58VA 21/22/28 86 FR 61858, Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA which is published in the Federal Register.

Veterans Service Organization (VSOs), State Approving Agencies (SAA), and VA Accredited Attorney or Claims Agents, share their own data when applying for a VA account (using VA Form 20- 8824E8824E) to access Veterans Benefits Administration (VBA) systems. All VSO-SAA Officials and Claims Agents sign the VA Rules of Behavior and are vetted the same as any other individual requesting internal VA Network access. A copy of the form VA Form 20- 8824E 8824Ecan be found at the following link:
http://vaww.va.gov/vaforms/Search_action.asp?FormNo=8824E&tkey=&Action=Search

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

If the requested information is not provided to CSS, the user will be denied access to systems. If a Veteran declines to provide information to the source system, this could result in a denial of benefits, if the VBA is unable to verify the Veteran's eligibility.

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

Any right to consent to particular uses of the information would be handled by the source systems that collect the information from the veteran. Individuals seeking information regarding access to and contesting of VA records from the source system may write, call or visit the nearest VA regional office. Address locations are listed in VA Appendix 1. Refer to VA SORN

Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA, SORN 58VA21/22/28(November 8, 2021).

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 to the veteran or employee. The public may not be aware the CSS system exists and the purpose for the CSS system.

Mitigation: The VA mitigates this risk by providing Veterans and other beneficiaries with multiple forms of notice of information collection, retention, and processing. Notice is provided, primarily, via 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.

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. See VA SORN Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA, SORN 58VA21/22/28(November 8, 2021).

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 correction of inaccurate or erroneous information would not occur within CSS, itself, as CSS does not store any PII or SPI. All data is stored in the VBA Corporate Database.

The Individuals seeking information regarding access to and contesting of VA records at the source system may write, call or visit the nearest VA regional office. Address locations are listed in VA Appendix 1. See VA SORN Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA, SORN 58VA21/22/28(November 8, 2021).

CSS Administrators and ISO have access to all CSS data. The end user access is restricted by the level of authority they require to perform their jobs. The CRP/BEP Customers include authorization at the application and function level. Users may have inquiry, update (sometimes sub-divided), or verifier authority to different screens. The only authorized users (routine-user) are the System Administrator and the Information System Security Officer (ISSO).

The SSN is used only for internal identification purposes. Usually, it is the ISSO who is first to notice a situation where the SSN or VA Claim Number in CSS does not match the access request form. ISSOs have “read-only” access. Administrators cannot modify their own security record. In no situation would the end-user for which the security record was created have access to their security record.

The ISSO is required to perform audits by crosschecking permissions approved on the VA FORM 20-8824E (Access form) against the actual permission entered into CSS. Any change to individual records would have to be made by contacting their VBA Regional Office.

Common Security Services (CSS) User Access Request VA FORM 20-8824E is completed in its entirety and resigned by the Business Owner, ISSO and the CSS System Administrator when new, updated and/or deletions to CSS account information is requested.

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.

CSS does not store or maintain any PII or SPI. All PII and SPI is housed within the VBA Corporate Database and is not part of the CSS application's accreditation boundary. Therefore, VBA application that contains the Veteran's record would provide instruction regarding record correction. Once the Veterans information is corrected within the appropriate VBA application the information would be updated in the VBA Corporate Database.

VA SORN Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA, SORN 58VA21/22/28(November 8, 2021), 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: http://benefits.va.gov/benefits/offices.asp."

CSS itself only collects information from external entities via form Common Security Services (CSS) User Access Request VA Form 20-8824E. If the information provided on form 8824-E does not match what is already stored in other applications and provided to the VBA Corporate Database, the individual will not be allowed access. In such case, the individual would need to correct their information, and submit a new form.

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.

CSS itself only collects information from external entities via form 8824E. If an individual is seeking a correction to their information, they would need to submit a new form.

The Veteran can also visit a VBA Regional Office, the VBA Internet Site, or call 1-888-442-4551 for assistance with this process.

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: This risk would fall on the VBA application to which the user is trying to access. CSS itself does not store any PII or SPI.

Mitigation: VA, SORN 58VA21/22/28 (November 8, 2021) 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.

Applicants must request access via VA FORM 20-8824E or electronically using CSEM. A series of verification and approval levels are set up to ensure the applicant's information is valid and management approves of the access.

Prior to receiving access, the user must complete and sign User Access Request Form. The user must complete, acknowledge, and electronic signs he/she will abide by the VA Rules of Behavior. The user also must complete mandatory security and privacy awareness training.

CSS Administrators and ISSO have access to all CSS data. The end user access is restricted by the level of authority they require to perform their jobs. The systems include authorization at the application and function level. Users may have inquiry, update (sometimes sub-divided), or verifier authority to different screens. The only authorized users (routine-user) are the System Administrator and the Information System Security Officer.
The SSN is used only for internal identification purposes. Usually, it is the Information Security Officer who is first to notice a situation where the SSN or VA Claim Number in CSS does not match BIRLS or the access request form. ISSOs have "read-only" access. Administrators cannot modify their own security record.

In no situation is the end-user for which the security record was created would ever have access to their security record.

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.

VA contractors do not have access to the CSS production environment and all PII is stored in the VBA Corporate Database, which is not part of the CSS accreditation boundary. The contractors that work on the VBA Corporate Database are vetted as follows:

- VBA VA contract employee access is verified through the Contracting Officer's Representative (COR) and other VA supervisory/administrative personnel before access is granted to any VA system.
- Contractor access is reviewed annually at a minimum.

- The contractors who provide support to the system are required to complete annual VA Privacy and Information Security and Rules of behavior training via the VA Talent Management System (TMS).
- All contractors are vetted using the VA background investigation process and must obtain the appropriate level background investigation for their role.
- Contractors with system administrative access are required to complete additional role-based training prior to gaining system administrator access.
- Generally, contracts are reviewed at the start of the initiation phase of acquisitions and again during procurement of option years by the Contracting Officer, Information System Security Officer, Privacy Officer, COR, Procurement Requestor/Program Manager and any other stakeholders required for approval of the acquisition.
- Contracts generally have an average duration of 1-3 years and may have option years stipulated in the original contract.

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

VA offers privacy and security training. Each program or system may offer training specific to the program or system that touches on information handling procedures and sensitivity of information. Please describe how individuals who have access to PII are trained to handle it appropriately. This question is related to privacy control AR-5, Privacy Awareness and Training.

Personnel that will be accessing information systems must read and acknowledge their receipt and acceptance of the VA National Rules of Behavior (ROB) or VA Contractor's ROB 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 re-affirm their acceptance annually as part of the security awareness training. Acceptance is obtained via electronic acknowledgment and is tracked through the TMS system. CSS employees must also 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,*
2. *The Security Plan Status Date,*
3. *The Authorization Status,*
4. *The Authorization Date,*
5. *The Authorization Termination Date,*
6. *The Risk Review Completion Date,*
7. *The FIPS 199 classification of the system (LOW/MODERATE/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.***

1. The Security Plan Status: Complete; Re-signed Annually
2. The Security Plan Status Date: 08-30-2021 - New SSP to be signed before expiration
3. The Authorization Status: ATO valid through 11-03-2022 – New ATO to be obtained before expiration.
4. The Authorization Date: 11-03-2021
5. The Authorization Termination Date: 11-03-2022
6. The Risk Review Completion Date: 09-14-2021
7. The FIPS 199 classification of the system: MODERATE.

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.

- The system does not utilize 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.

- N/A The system does not utilize 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.

- N/A The system does not utilize 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.

- N/A The system does not utilize 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).

- N/A The system does not utilize Robotics Process Automation (RPA).

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.

JEAN-CLAUDE WICKS

Digitally signed by JEAN-CLAUDE WICKS
Date: 2023.01.03 05:58:12 -07'00'

Privacy Officer, Jean-Claude Wicks

Tamer F. Ahmed 531244

Digitally signed by Tamer F. Ahmed 531244
Date: 2023.01.03 08:10:02 -05'00'

Information System Security Officer, Tamer Ahmed

Lindsay S Tucker 169804

Digitally signed by Lindsay S Tucker 169804
Date: 2022.12.29 11:23:39 -06'00'

Information System Owner, Lindsay Tucker

APPENDIX A-6.1

Privacy notice is provided via the Internet site (http://www.va.gov/privacy/) and the SORN 58VA 21/22/28 86 FR 61858, Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA which is published in the Federal Register.
https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24372.pdf

Veterans Service Organization (VSOs), State Approving Agencies (SAA), and VA Accredited Attorney or Claims Agents, share their own data when applying for a VA account (using VA Form 20- 8824E8824E) - VA Form 20- 8824E 8824Ecan be found at the following link:
http://vaww.va.gov/vaforms/Search_action.asp?FormNo=8824E&tkey=&Action=Search