Privacy Impact Assessment for the VA IT System called:

Personnel Information Exchange System (PIES)

Veterans Benefits Administration (VBA) Corporate Applications

Date PIA submitted for review:

09/29/2020

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Simon Caines	Simon.Caines@va.gov	(202) 461-9468
Information System Security Officer (ISSO)	Tamer Ahmed	Tamer.Ahmed@va.gov	(202) 461-9306
Information System Owner	Gary Dameron	Gary.Dameron2@va.gov	(202) 492-1441

Abstract

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

Personnel Information Exchange System (PIES) is a client/server-based application, falls under VBA Corporate Applications. PIES was designed to improve the quality and timeliness of requesting veteran information from outside agencies. The information gained from these requests is used to process claims for compensation, pension, education, burial benefits, and loan guaranty. These improvements are achieved by automating and standardizing the data requests, improved routing, request tracking, standard output generation processes, and process metrics involved with claims development. PIES is an automated system that manages the requests for veteran information that is required to develop, and process claims more efficiently. PIES consist of two executable programs: PIES Create Application was developed for users at Regional Office (RO) and PIES Respond application was developed for users at VA Liaison Office (formally the Record Management Center) to create and respond to 3101 requests (VBA information request form). No existing PTA for PIES. PIES was formerly under Corporate Database (CRP) Authorization Boundary. It is now separated and a standalone system that requires its own Authorization.

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 Personnel Information Exchange System (PIES) consists of software modules which reside and execute on several VBA hardware platforms consisting of the SUN host processors, the Local Area Network (LAN) file server hosts and the PC workstation. PIES was developed using the VBA Stage I development environment which includes Oracle Relational Database Management Systems (RDBMS), Oracle Tuxedo (and the accompanying VBA Tuxedo Wrapper Application Programming Interface (APIs)) and the Microsoft Visual Basic development tools.

The purpose of the PIES system is to manage formal requests for veteran military service data maintained by the Department of Veteran Affairs Liaison Office (VALO) and the NARA's National Personnel Records Center. At the VBA regional offices, the adjudication process may require additional service or medical information which is recorded in the veteran's military folder often residing at VALO or NPRC. A Regional Office (RO) user submits a formal request to the PIES system for the records centers to respond when the veteran folder is located. The VALO and NPRC have interfaces to PIES to formally respond to outstanding requests.

The current PIES system is dependent on the CSS package. PIES is integrated with the CSS workstation security Dynamic Link Library (DLL) or the Sensitive File Check module on the SUN hosts. The PIES workstation programs display a VBA CSS (Common Security Service) User Authentication box for users to supply their Personal Identity Verification (PIV) Card network password and station code to access the PIES application and database objects.

The PIES Tuxedo database objects were built with and depend on the VBA Tuxedo Wrapper APIs. The PIES database server modules utilize the Tuxedo server which also must be built/executing with the Tuxedo Wrapper APIs.

The PIES database does not use or depend on the VBA Corporate Data Model. The PIES database definition uses the same naming conventions and column sizes as the VBA Corporate Data Model but does not share any tables or data elements.

The PIES system utilizes the Beneficiary Identification Record Locator System (BIRLS) to aid in the creation of a 3101 request. PIES accesses BIRLS from its database objects residing on the Sun host. The *PIES Create* workstation program used by regional offices performs an interactive query to the BIRLS system for 3101 requests submitted to the PIES database. The *PIES Respond* workstation program used by record centers (VALO and NPRC) perform an interactive query and update to the BIRLS system. The PIES access to BIRLS is primarily during daytime VBA operation hours.

The PIES system must access the NARA (National Archives and Records Administration) MPR Registry database to fulfill 3101 requests. Access to this database is from PIES Tuxedo server, using a web-service, to access NARA's MPR (Military Personnel Record) registry database located on NARA's CMRS (Case Management and Reporting System) system in College Park, Maryland. The message sent to the MPR Registry database consists of the required headers and the Social Security Number or Service Number to be searched upon. NARA provide a WSDL (Web Service Definition Language) file of the MPR registry return data.

An ECS job is scheduled to initiate the call from the batch program over an encrypted link (SSL (Secure Socket Layer)). The Tuxedo batch program initiating the request it will appear that it is calling another function. Secured Web Services can be used where User ID and Password are part of Simple Object Access Protocol (SOAP) message. NARA internally uses Lightweight Directory Access Protocol (LDAP) authentication for further processing.

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.

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
- ☐ Other Unique Identifying Number (list below)

Place of Birth, Date of Death, service number, Enter on Duty date (EOD), Release from active duty date (RAD), Character of Discharge (COD), branch of service, assigned separation reason, pay grade.

PII Mapping of Components

Personnel Information Exchange System (PIES) consists of 3 key components. Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by PIES and the reasons for the collection of the PII are in the table below.

PII Mapped to Components

PII Mapped to Components

Components of the information system (servers) 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
VBACorporateApplication1	Yes	Yes	Name, Social Security Number, Date of Birth, Place of	Provides/tracks Veterans' supporting information and folders for claims and requests	Database is behind a firewall, access via CSS (common

			Birth, Date of Death, service number, Enter on Duty date (EOD), Release from active duty date (RAD), Character of Discharge (COD), branch of service, pay grade.		**security system)**
VBACorporateApplication2	**Yes**	**Yes**	**Name, Social Security Number, Date of Birth, Place of Birth, Date of Death, service number, Enter on Duty date (EOD), Release from active duty date (RAD), Character of Discharge (COD), branch of service, pay grade**.	**Provides/tracks Veterans' supporting information and folders for claims and requests**	**Database is behind a firewall, access via CSS (common security system)**
VBACorporateApplication3	**Yes**	**Yes**	**Name, Social Security**	**Provides/tracks Veterans' supporting**	**Database is behind a firewall,**

			Number, Date of Birth, Place of Birth, Date of Death, service number, Enter on Duty date (EOD), Release from active duty date (RAD), Character of Discharge (COD), branch of service, pay grade.	**information and folders for claims and requests**	**access via CSS (common security system)**
VBAProduction	**Yes**	**Yes**	**Name, Social Security Number, Date of Birth, Place of Birth, Date of Death, service number, Enter on Duty date (EOD), Release from active duty date (RAD), Character of Discharge (COD), branch of**	**Provides/tracks Veterans' supporting information and folders for claims and requests**	**Database is behind a firewall, access via CSS (common security system)**

			service, pay grade.		
BIRLS	**Yes**	**Yes**	**Name, Social Security Number, Date of Birth, Mailing Address, Zip Code, Phone Numbers, Email Address, Financial Account Information, Health Insurance Beneficiary Numbers, Current Medications, Previous Medical Records**	**Provides/tracks Veterans' supporting information and folders for claims and requests**	**BIRLS database is behind a VA approve firewall only access via CSS (common security system)**
PIES/NARA's CMRS Interface	**Yes**	**Yes**	**PIES to NARA SSN and service numbers.** **NARA to PIES, SSN, service number, Name, Service code and Registry information**	**Provides/tracks Veterans' supporting information and folders for claims and requests**	**Site to site VPN Secured connection**

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.

When a veteran submits a claim, the Veterans Service Representative (VSR) or other user at the RO will open the PIES Create program. Once the application is launched, the VSR enters the Veteran's information for a search, PIES will search the Beneficiary Identification Records Locator System (BIRLS) database for veteran's information and the PIES database for existing 3101s. If there is data in BIRLS for the requested veteran, that information is used to populate the PIES 3101 screens. The user may edit the information as needed. If a BIRLS record is not found, or if BIRLS is not available, the user can create a new 3101. After all the required information has been entered, the user submits the 3101 to the PIES database. The PIES application, nightly batch job, then makes a logical decision as to which depository to address the request. The 3101 request is then forwarded to the VALO staff at the NPRC in St Louis for direct response or VA personnel at the VA Liaison Office in St Louis.

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.

The purpose of the PIES system is to manage formal requests for veteran military service data maintained by the Department of Veteran Affairs Liaison Office and the NARA's National Personnel Records Center. At the VBA regional offices, the adjudication process may require

additional service or medical information which is recorded in the veteran's military folder often residing at VALO or NPRC. A RO user submits a formal request to the PIES system for the records centers to respond when the veteran folder is located.

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 publicly 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 Name, SSN, Insurance number and Date of Birth information are used to locate the Veteran's information in the VA system so the VSR (Veteran Service Representative) can review the Veteran's military history to determine eligibility of benefits. As stated in SORN 58VA21/22/28, 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 provide the legal authority for operating the CBA C&P Corporate Applications. stays in sync with the BIRLS, which use SSN to distinguish the veteran's record.

1.5 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 PIES system front end has several edits on required fields, which checks for accuracy prior to the request being submitted. Users can also modify the BIRLS records for accuracy. For the PIES/NARA's CMRS interface, data is not check for accuracy.

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

Title 38 United States Code section 501(a) and Chapters 11, 13, 15, 18, 23, 30, 31, 32, 34, 35, 36, 39, 51, 53, 55. The SSN is used to identify the Veteran.38 U.S.C. § 5106 (Department of Veterans Affairs (DVA statute) requires the head of any Federal department or agency, including SSA, to provide information, including SSNs, to the DVA for purposes of determining eligibility for or amount of VA benefits, or verifying other information with respect thereto. SSNs are used extensively through the Loan Guarantee (LGY) Web Applications. End user SSNs are used to uniquely identify registered users. Veteran SSNs are used to validate eligibility requirements and rating information from the external systems. SORN: Loan Guaranty Home, Condominium and Manufactured Home Loan Applicants Records, Specially Adapted Housing Applicant Records and Vendee Loan Applicant Records- VA 55VA26 http://www.gpo.gov/fdsys/pkg/FR-2014-01-23/pdf/2014-01286.pdf by the Privacy Act of 1974, 5 U.S.C. 552a(E)(4 6, 5 U.S.C. 552a(R)and OMB 59 FR 37906, 3791618, July 25, 1994.

1.7 <u>PRIVACY IMPACT ASSESSMENT: Characterization of the information</u>

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:

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

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

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

<u>Principle of Data Quality and Integrity:</u> 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: PIES collect Personally Identifiable Information (PII) and other sensitive information. If this information is breached or accidentally released to inappropriate parties or the public, it could result in financial, personal, and/or emotional harm to the individuals whose information is contained in the system.

Mitigation: All employees with access to Veteran's information are required to complete the VA Privacy, Information Security Awareness training and Rules of Behavior annually. The Department of Veterans Affairs is careful to only collect the information necessary to identify the parties involved in an incident, identify potential issues and concerns, and offer assistance to the affected parties so that they may find the help they need to get through their crisis. By only collecting the minimum necessary information, the VA is able to better protect the individual's information.

Section 2. Uses of the Information

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

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

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

Name - Veteran's Identification
Social Security Number - Used to verify Veteran identity and as a file number for Veteran
Date of Birth – Used to verify Veteran identity
Service Number – Used to verify Veteran identity
Enter on Duty (EOD) – Used to verify Veteran Military service
Release from Active Duty (RAD) – Used to verify Veteran Military service
Branch of Service – Used to verify Veteran Military service
Pay Grade – Used to verify Veteran Military service
Health Insurance Beneficiary Numbers –
Character of Discharge (COD) –
Assigned separation reason-

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

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

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

The PIES GUI front end does not analyze, accumulate or interpret the data received or provided; it merely displays it from the database.

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.

Users are trained on 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 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 - Veteran's Identification
Social Security Number - Used to verify Veteran identity and as a file number for Veteran
Date of Birth – Used to verify Veteran identity
Service Number – Used to verify Veteran identity
Enter on Duty (EOD) – Used to verify Veteran Military service
Release from Active Duty (RAD) – Used to verify Veteran Military service
Branch of Service – Used to verify Veteran Military service
Pay Grade – Used to verify Veteran Military service
Health Insurance Beneficiary Numbers –
Character of Discharge (COD) –
Assigned separation reason-

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.

The information is retrieved directly from these records are retained in accordance with the General Records Schedule Sections 3.0 Technology and 4.0 Information Management, approved by National
Archives and Records Administration (NARA). http://www.archives.gov/records-mgmt/grs.html

Retention of Records is expected to be 75 years. The information is retained following the policies and schedules of VA's Records management Service and NARA in "Department of Veterans Affairs Records Control Schedule 10-1". Record Control Schedule 10-1 can be found at the following link:
https://www.va.gov/vhapublications/RCS10/rcs10-1.pdf"

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.

Paper documents are destroyed to an unreadable state in accordance with the Department of Veterans' Affairs VA Directive 6371, (April 8, 2014), https://www.va.gov/vapubs

Electronic data and files of any type, including Protected Health Information (PHI), Sensitive Personal Information (SPI), Human Resources records, and more are destroyed in accordance with the **Department of Veterans' Affairs Handbook 6500.1, Electronic Media Sanitization** (November 3, 2008),

https://www.va.gov/vapubs. When required, this data is deleted from their file location and then permanently deleted from the deleted items,or Recycle bin. Magnetic media is wiped and sent out for destruction per VA Handbook 6500.1. Digital media is shredded or sent out for destruction per VA Handbook 6500.1.

Additionally, this system follows Field Security Service (FSS) Bulletin #176 dated April 9, 2014 for Media Sanitization Program, SOPs - FSS - All Documents as well as FSS Standard Operating Procedures (SOP) MP-6 Electronic Media Sanitization.

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

PIES Database records are retained indefinitely.

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

The PIES system does not use PII for training and research. If PII information is used in PIES for testing, the record is deleted to minimize the risks associated with unauthorized disclosure and misuse of the information.

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

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

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

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

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

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

Follow the format below:

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

Mitigation: To mitigate the risk posed by information retention, adhere to the NARA General Records Schedule. When the retention date is reached for a record, the individual information is carefully disposed of by the determined method as described in General Records Schedule 3.0.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

The following questions are intended to define the scope of information sharing/receiving/transmitting within VA. NOTE: Question 5 on Privacy Threshold Analysis should be used to answer this question.

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?

Identify and list the names of any program offices, contractor-supported IT systems, and any other organization or IT system within VA with which information is shared.

State the purpose for the internal sharing. If you have specific authority to share the information, provide a citation to the authority.

For each interface with a system outside your program office, state what specific data elements (PII/PHI) are shared with the specific program office, contractor-supported IT system, and any other organization or IT system within VA.

Describe how the information is transmitted. For example, is the information transmitted electronically, by paper, or by some other means? Is the information shared in bulk, on a case-by-case basis, or does the sharing partner have direct access to the information?
This question is related to privacy controls AP-2, Purpose Specification, AR-3, Privacy Requirements for Contractors and Service Providers, AR-8, Accounting of Disclosures, TR-1, Privacy Notice, and UL-1, Internal Use.

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific data element types such as PII/PHI that are shared/received with the Program Office or IT system***	***Describe the method of transmittal***
BIRLS	The purpose of this information is to verify veteran Military service	Name, Social Security Number, Date of Birth, Mailing Address, Zip Code, Phone Numbers, Email Address, Financial Account Information, Health Insurance Beneficiary Numbers, Current Medications, Previous Medical Records	Message transaction
VA Records Management Center (RMC).	The purpose of this information is to verify veteran Military service	Name, Social Security Number, Date of Birth, Mailing Address, Zip Code, Phone Numbers, Email Address, Financial Account Information, Health Insurance Beneficiary Numbers, Current Medications, Previous Medical Records	Electronic transmission

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: The sharing of data is necessary for the support benefits claim processing. However, There is a risk that information could be shared with an inappropriate VA organization.

Mitigation: Consent for use of PII data is signed by completion of benefits forms by the Veteran. The principle of need to know is strictly adhered to. Only personnel with a clear business purpose are allowed access to the system and information contained within. Review of access to all systems are done on a quarterly basis by the ISO and the security engineer. Clearance is required for each person accessing the system. 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: This question is #7 in the Privacy Threshold Analysis.

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 data element types such as PII/PHI that are shared/received 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***
PIES/NARA Interface	The purpose of this information is to correctly process the veteran claim.	SSN & Service Number / MPR Registry.	ISA (Interconnection Security Agreement)/MOU (memorandum of understanding)	Two-way Site to Site VPN

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

The Interconnection Security Agreement and Memorandum of Understanding notes the agreement between the Veterans Benefits Administration (VBA) and National Archives Records Administration (NARA) regarding the development, management, operation, and security of a connection between VBA Corporate Applications and Case Management and Reporting System (CMRS).

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

Discuss whether access controls have been implemented and whether audit logs are regularly reviewed to ensure appropriate sharing outside of the Department. For example, is there a Memorandum Of Understanding (MOU), contract, or agreement in place with outside agencies or foreign governments.
Discuss how the sharing of information outside of the Department is compatible with the stated purpose and use of the original collection.
This question is related to privacy control AR-2, Privacy Impact and Risk Assessment, AR-3, Privacy Requirements for Contractors and Service Providers, and AR-4, Privacy Monitoring and Auditing

Follow the format below:
Privacy Risk: There is a risk that information could be accessed by unauthorized individuals when sharing externally.

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. PIES adhere to all information security requirements instituted by the VBA. 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 user ID and password, and using a Personal Identity Verification (PIV) card. This ensures the identity of the user by requiring two-factor authentication.

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.

PIES do not provide Notice of Privacy Practice to Veterans when we make a PIES request to NARA for their records. When the Veteran signs the VA Form 21-526EZ, we have consent to request their records from NARA. An ISO and MOU were completed for the PIES NARA interface. VA consistently publishes all SORNS to the Federal Register as dictated by law and VA Policy. VA requires the Administration and Staff Offices to put forth for approval and publication all notice for their respective Privacy Act system of records. VBA routinely updates SORN for altered system of record that include major changes or changes in the routine use. VBA ensuring that the required notice is given with requests for Social Security Numbers, and that a Privacy Act statement appears on each applicable form or accompanying instruction sheet collecting information that is going into a Privacy Act system of records (see 5 USC 552a(e)(3)). SORN: Loan Guaranty Home, Condominium and Manufactured Home Loan Applicants Records, Specially Adapted Housing Applicant Records and Vendee Loan Applicant Records-VA 55VA26 https://www.oprm.va.gov/docs/Current_SORN_List_8_25_20.pdf

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

A Veteran may have the opportunity or notice of the right to decline to provide information to the source systems that collects the information from the Veteran. By declining to supply information to the source system, the Veteran would also be declining the information to the PIES system and other claim processing systems.

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

Veterans may have the opportunity or notice of the right to decline to provide information to the source systems that collects the information from the Veteran. By declining to supply information, this will delay processing the veteran claim.

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: There is a risk that an individual may not receive notice that their information is being collected, maintained, processed, or disseminated.

Mitigation: The VA mitigates this risk by providing veterans and other beneficiaries with multiple forms of notice of information collection, retention, and processing. The main forms of notice are discussed in 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.

VBA provides individuals the right of access, under the Privacy Act, only to his or her records which are not exempt pursuant to subsections (j) and (k) of the Privacy Act. Access is given only to information which is retrieved by the individual's own personal identifier(s). Each VBA SORN contains "Notification" and "Access" sections that indicate the official to whom such requests should be directed. An individual wanting notification or access, including contesting the record, should mail or deliver a request to the office identified in the SORN. If an individual does not know the "office concerned," the request may be addressed to the PO or FOIA/PO of any VA field station or the Department of Veterans Affairs Central Office, 810 Vermont Avenue, NW, Washington, DC 20420. Each VBA SORN contains "Notification" and "Access" sections that indicate the official to whom such requests should be directed. An individual wanting notification or access, including contesting the record, should mail or deliver a request to the office identified in the SORN. If an individual does not know the "office concerned," the request may be addressed to the PO or FOIA/PO of any VA field station or the Department of Veterans Affairs Central Office, 810 Vermont Avenue, NW, Washington, DC 20420. VBA Privacy has submitted draft policy guidance to address the processing of Privacy Act requests. The policy draft is currently being reviewed by VBA Leadership.

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.

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. 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 is 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.

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.

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. An approved VA notification of amendment form letter may be used for this purpose. (5) If it is determined not to grant all or any portion of the request to amend a record, the VA official will promptly notify the individual in writing.

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.

The individual will be advised of his or her right to file a concise statement of reasons for disagreeing with the refusal to amend.

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 a Veteran may not know how to obtain access to their records or how to request corrections to their records.

Mitigation: Individuals are allowed to provide updated information for their records by submitting new forms or correspondence and indicating to the VA that the new information supersedes the previous data.

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 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 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 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. ISOs 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 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.

OIT provides basic security awareness training to all information system users (including managers, senior executives, and contractors) of VA information systems or VA sensitive information as part of initial training for new users, when required by system changes and annually thereafter. 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) and they are required to sign Non-Disclosure Agreement (NDA). All contractors are vetted using the VA background investigation process and must obtain the appropriate level background investigation for their role. Contractors with systems 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 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. All VA employees must complete annual Privacy and Security training. Users agree to comply with all terms and conditions of the National Rules of Behavior, by signing a certificate of training at the end of the training session. HIPAA training is a standard requirement.

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

If Yes, provide:

1. *The date the Authority to Operate (ATO) was granted,*
2. *Whether it was a full ATO or ATO with Conditions,*
3. *The amount of time the ATO was granted for, and*
4. *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 date the Authority to Operate (ATO) was granted,*
   09 April, 2020*.*

2. *Whether it was a full ATO or ATO with Conditions,*
   ATO with Condition
3. *The amount of time the ATO was granted for, and*
   12 months*.*
4. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH).*
   Moderate

Section 9. 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

APPENDIX A-6.1

Please provide a link to the notice or verbiage referred to in Section 6 (a notice may include a posted privacy policy, a Privacy Act notice on forms).

http://www.gpo.gov/fdsys/pkg/FR-2014-01-23/pdf/2014-01286.pdf
https://www.oprm.va.gov/docs/Current_SORN_List_8_25_20.pdf"

Signature of Responsible Officials

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

Simon K. Caines 3430973

Digitally signed by Simon K. Caines 3430973
Date: 2020.10.26 08:21:00 -04'00'

PO, Simon Caines

Tamer F. Ahmed 531244

Digitally signed by Tamer F. Ahmed 531244
Date: 2020.10.26 10:08:14 -04'00'

Information Security Systems Officer, Tamer Ahmed

Gary W. Dameron 101941

Digitally signed by Gary W. Dameron 101941
Date: 2020.10.26 10:23:16 -04'00'

System Owner, Gary Dameron