Privacy Impact Assessment for the VA IT System called:

EDUCATION CALL CENTER (ECC)
CUSTOMER RELATIONSHIP MANAGEMENT (CRM)

VETERAN EXPERIENCE SERVICES (VES)
VETERANS BENEFITS ADMINISTRATION (VBA)

Date PIA submitted for review:

JUNE 15, 2022

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Bertha. L. Brown	Bertha. Brown@va.gov	202-461-9740
Information System Security Officer (ISSO)	Thomas Orler	Thomas.Orler@va.gov	708-938-1247
Information System Owner	Stefano Masi	Stefano.Masi@va.gov	860-681-9927

Abstract

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

The U.S. Department of Veterans Affairs (VA) Veterans Benefits Administration (VBA) provides benefits and services to eligible Veterans and their dependents. The Customer Relationship Management (CRM) implementation for the Education Call Center (ECC) focuses on delivering capabilities to the ECC CRM Customer Service Representatives (CSRs) to provide world-class customer service to the VA education benefit recipients. This product utilizes Microsoft Dynamics 365 Software as a Service (SaaS) that leverages the Platform as a Service (PaaS) interface platform to interface with VA Services in the Cloud. ECC CRM functionality provides a consolidated way to answer, track, and report calls from Veterans, beneficiaries, and school officials about education benefits for Veterans.

Overview

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

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

The ECC CRM application is owned by U.S. Department of Veterans Affairs (VA) Veterans Benefits Administration (VBA) and maintained by the Enterprise Portfolio Management

Division (EPMD) Benefits Appeals and Memorials (BAM) Portfolio. The Customer Relationship Management (CRM) implementation for the Education Call Center (ECC) focuses on delivering capabilities to the ECC Customer Service Representatives (CSRs) to provide world-class customer service to the VA education benefit recipients.

The CSRs ask for the Social Security Number (SSN) with the callers, and use that to query the CRM. The CRM searches the Personal Accountability & Integrity (PA&I), Benefits Delivery Network (BDN), and Digital GI Bill (formerly Long Term Solution [LTS]), and outputs the benefits tied with the SSN in the search results which is used to verify the caller, and their benefits. Once a benefit is selected the CRM opens a form to document the reasons for the call, resolutions provided if any. Once this phone call form is saved, CSRs can record if any follow up is needed by creating a case linked to the call. The Education Call Center receives roughly ten thousand calls (10,000) a day and the CSRs document each of those calls.

The system helps both VA education benefits beneficiaries and the school officials who correspond with the beneficiaries. The CRM is not a system of record about the beneficiaries or their benefits. It only records the phone contact made by the beneficiaries or their representatives to the call center, and screen-hosts the commonly used VA applications by the CSRs which are BDN, Flight, On-the-Job Training, Correspondence and Apprenticeship System (FOCAS), Digital GI Bill (DGI), SHARE (not an acronym), The Image Management System (TIMS), Veteran Information Solution Revised (VIS-r), and Web Enabled Approval Management System (WEAMS). So, the CRM serves as one stop shop for the CSRs to access all the information that they may need about the beneficiaries. Logics are also built in the system which causes subset of the VA systems identified to be opened in the CRM when CSR's select a call reason saving CSRs time to accumulate information to help the caller.

Approximately, one million (1,000,000) beneficiaries are served by VA Education programs, which provides Veterans, Service members, reservists, and certain family members of Veterans with educational resources to supplement opportunities missed because of military service. These programs are also meant to help the Armed Forces both recruit and retain members. For members of the Armed Forces, VA educational benefits assist in the readjustment to civilian life. On a broader scale, educationalbenefits are meant to enhance the Nation's competitiveness through the development of a more highly educated and more productive workforce. The ECC application has access to SSN, and benefits information of the one million (1,000,000) VA education program beneficiaries, and saves every contact made by the beneficiaries to the call center.

The CRM software for the ECC includes an application that the CSRs have to install in their desktop. All CSRs dedicated for the ECC are located in Muskogee, OK which falls under Region 5, i.e. the ECC application is operated only in one site. The ECC application has a log of each call received by the call center.

Citation of the legal authority to operate the IT system is "Title 38, United States Code, Section 501 –Veterans' Benefits" and "SORN 58 VA21/22/28, 38 USC 1781, 1802, 1724, 1728, 1703, 1725, 1728, 1781, 1803 and Public Law 103-446 section 107".

Completion of this PIA is not expected to result in circumstances that require changes to business processes or technology changes.

VA Office of Information & Technology (OIT), Benefits, Appeals and Memorial (BAM), Enterprise Portfolio Management Division (EPMD) proposes a new SORN 191VA005 for the BAM CRM Application Framework containing VBA records for CRM applications, including ECC CRM.

The VA is the owner of all data in the ECC CRM application, including PII, as established under the Microsoft Dynamics 365 Cloud Services contract. The Dell/Microsoft Enterprise Agreement contract information is as follows: Contract Number: 47QTCA22D003G-36C10B22F0089. The period of performance is from March 29, 2022 through March 31, 2024.

The ECC CRM application is hosted on Microsoft - Azure Government (includes Dynamics 365). It is a Software-as-a-Service (SaaS) offering as defined in NIST SP800-145. Both the primary and backup data centers are owned by Microsoft, who is the VA contracted Cloud Service Provider (CSP) at those sites with direct connections to the VA Trusted Internet Connection (TIC) Gateway from each respective location.

The magnitude of potential harm to the Veteran or Beneficiary if privacy-related data is disclosed is moderate due to the potential for identity theft. An unauthorized privacy-related data disclosure could negatively affect the reputation of both the CSP and the VA, as well as cause a reduction of public trust.

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)

Other Unique Identifying Information:

- Eligibility Status
- Veteran Call History
- Electronic data interchange personal identifier (EDIPI)
- Facility and School Certifying Official (SCO) information
- Enrollment Information for On-the-Job Training Programs
- Payment- financial information
- Debt- financial information
- Beneficiary Profile Information

PII Mapping of Components

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

PII Mapped to Components

Note: Due to the PIA being a public facing document, please do not include the server names in the table. The first table of 3.9 in the PTA should be used to answer this question.

PII Mapped to Components

Components	Does this system collect PII? (Yes/No)	Does this system store	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards

		PII? (Yes/No)			
Interaction	Yes	Yes	Name, SSN, DOB, Phone Number(s), Fax Number, TIN, EDIPI	Caller identification; Veteran identity verification	Access to system is limited; access requires PIV; access to system and components shall be audited
Request	Yes	Yes	Name, SSN, DOB, Phone Number(s), Fax Number, TIN, EDIPI	Veteran identity verification; Customer service (retrieval of benefits, beneficiary, school information, etc.)	Access to system is limited; access requires PIV; access to system and components shall be audited
Veteran Record	Yes	Yes	Name, SSN, DOB, Phone Number(s), EDIPI, ICN	Veteran identity verification; Customer service (retrieval of benefits, beneficiary, school information, etc.)	Access to system is limited; access requires PIV; access to system and components shall be audited

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.

The primary sources of information in the ECC CRM systems are from the internal VBA systems and direct Veteran interaction/confirmation via telephone communication with the CSRs. Information is pulled from MPI, BDN, DGI, SHARE, TIMS, WEAMS, and VIS-r to ensure the CSRs receive all information necessary to assist the Veteran. Information can also be verified and updated with the Veteran during the telephone interaction.

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.

Performing a search against Master Person Index (MPI), BDN, DGI, and the Performance Analysis & Integrity (PA&I) database returns the facility, SSN, and Date of Birth (DOB) for the caller. Demographics, service connected information, insurance information, notes, and education information is pulled via interface from the Corporate Data Warehouse (CDW). Any request that requires information pulls it via the specified interface when that request is opened and clears the cache of data when it is closed. Notes can be added via the CRM and used to update as signed notes. Table 1 shows various business processes that result in information collection.

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.

All systems utilized by ECC CRM perform their own data validation processes. The ECC CRM system relies on the integrated systems to provide data and so therefore ECC CRM does not run extra validation and only display's the data from the external systems therefore, it is assumed the data has already been validated prior to its collection and usage. The CRM system is used to display vital information for completing tasks such as answering a caller's question, recording an interaction, adding notes.

ECC CRM application does not provide the CSRs ability to make any corrections in the integrated applications. It is outside the scope of the ECC application to make corrections in the source applications (MPI, BDN, DGI, Share, VIS-r, WEAMS, FOCAS, and TIMS), i.e., the data from

where the CRM is pulling the data from. The CSRs have to log into the integrated applications or open incidents to make any corrections.

1.5 What specific legal authorities, arrangements, and agreements defined the collection of information?

List the full legal authority for operating the system, specifically the authority to collect the information listed in question 1.1. Provide the authorities in a manner understandable to any potential reader, i.e., do not simply provide a legal citation; use statute names or regulations in addition to citations. Legal authorities include Federal laws, regulations, statutes, and Executive Orders.
This question is related to privacy control AP-1, Authority to Collect

The ECC CRM application complies with the following Federal regulations and/or Departmental policies and guidelines, as follows:

- Title 38, United States Code, Section 501-Veterans' Benefits
- System of Records 58VA21/22/28 – Compensation, Pension, Education, and Rehabilitation Records -VA
- Title 38, United States Code, Section 501- Veterans' Benefits
- Join Commission National Patient Safety Goals- Goal 1: Improve the accuracy of patient identification
- VHA Directive 1906- Data Quality Requirements for Healthcare Identity Management and the Master Veterans Index Functions
- VHA Directive 2009-021 Data Entry Requirements for Administrative Data
- VHA Directive 2006-036 Data Quality Requirements for Identity Management and the Master Patient Index Functions
- VHA Directive 2007-037 Identity Authentication for Health Care Services
- Office of Management and Budget (OMB) Circular A-130, Management of Federal Information Resources, Appendix III, November 2000
- VA Directive 6300, Records and Information Management

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: Data pulled by the ECC CRM application contains PII, and other sensitive information. Due to the highly sensitive nature of this data, there is a risk that, if the data were accessed by an unauthorized individual or otherwise breached, serious harm or even identity theft may result.

Mitigation: The ECC CRM application ensures strict access to information by enforcing thorough access control and requirements for end users. As a part of our access management activities, the following remote access security capabilities are in place: multi-factor authentication, individual administrator user IDs and access based on need, and restricted remote access devices for specified privileged users. ECC CRM limits access rights and controls only to valid end users. There are rigorous security monitoring controls to prevent unauthorized access and intrusion, and to protect all information. Furthermore, all end users are required to take Privacy, HIPAA, and information security training annually. The VA IT office is responsible in assuring safeguards for the PII.

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
- Mailing Address: Used to correspond with the Veteran
- Zip Code: Part of the mailing address
- Phone Number(s): Used to correspond with the Veteran
- Email Address: Used to correspond with the Veteran
- Emergency Contact Information (Name, Phone Number, etc. of a different individual): used in emergencies to contact the Veteran
- Eligibility Status: Used to provide relevant information on entitlement

- Next of Kin (NOK) Information: Used in emergency to contact the Veteran
- Veteran Call History: Used to provide call development and resolution data
- ICN: Used to identify veterans and beneficiary records between systems

Interfaces with BDN, DGI, and VIS/VIS-r (Veteran demographics) to provide dynamically constructed data feeds to help the user complete his or her work. The data is cached and displayed during the session, allowing the user to interact in a meaningful manner (the user can sort, filter, and search through datasets for specific information). When the session is complete and has ended, the cache is cleared; the bulk of the data used during the session is not stored. Only minimal, critical call information is retained by the CRM, as the system of record for phone interactions, giving management the ability to report on types of calls, first call resolution, and time to solve.

The information listed below is transmitted from the VBA systems and is pulled into the ECC CRM application to verify Veteran identity and assist with telephone inquiries.

- Full Name
- Social Security Number (SSN)
- Date of Birth (DOB)
- Mailing Address
- Zip Code
- Phone Number(s)
- Email Address
- Emergency Contact Information (Name, Phone Number, etc. of a different individual)
- Eligibility Status
- Next of Kin (NOK) Information
- Veteran Call History

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

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

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

The ECC CRM application has out-of-the-box reporting capabilities that can create reports to analyze data in the ECC CRM application. Charts can also be created from the data and/or list information on a dashboard. This is the only data analysis tool being used by the ECC CRM application this time.

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?

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

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

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

Personnel accessing information systems must read and acknowledge their receipt and acceptance of the VA National Rules of Behavior (ROB) or VA Contractor's ROB 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). The rules state the terms and conditions that apply to personnel who are provided access to, or use of, information, including VA sensitive information, or VA information systems, such as no expectation of privacy, and acceptance of monitoring of actions while accessing the system. 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 obtained through electronic acknowledgment is tracked through the TMS system. All VA employees must complete annual Privacy and Security training. ECC users agree to comply with all terms and conditions of the VA National ROB by signing a certificate of training at the end of the training session.

All individuals requesting developer access are required to complete all VA trainings (VA Privacy and Information Security Awareness and Rules of Behavior Training, Privacy and HIPAA Focused Training and Information Security for IT Specialists Training), and must be authorized by a VA Project Manager. To ensure that this requirement is met, the designated CRM Project point of contact (POC) must submit a signed Access Request From for an individual or a group. At minimum, the following information should be provided for each VA Project Team member requesting access to the ECC Environments: First Name, Last Name, Primary E-mail, Main Phone, Manager, Current on VA Training, VA Employee or Contractor, VA Active Directory Username, Environment, Access Permissions, and Contract End date. Additionally, ECC CRM implemented two factor authentication which requires agents to use VA PIV cards to access the system.

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

Access to PII is limited by the ECC CRM application to only those data items deemed necessary for an ECC CRM Agent to perform their job, as determined by their management team and their job description. System documentation includes detailed system design and user guides that specify those areas of the system that contain PII and PHI, as well as how it is to be used by the agent. Additionally, user roles are implemented to restrict user's access to only the specific information required to perform their job function. Roles within the system are determined and requested by Call Center supervisors (Senior Program Analyst or higher). User access is provided by ECC CRM System Administrators following receipt of request from appropriate individuals.

VBA ensures that the practices stated in the PIA are reinforced by requiring Contractors and VA employees to complete all VA trainings: VA Privacy and Information Security Awareness and rules of Behavior Training, and Privacy and HIPAA focused training. Contractors and VA employees are required to agree to all rules and regulations outlined in trainings, along with any consequences that may arise if failure to comply.

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

- Full Name
- Social Security Number (SSN)
- Date of Birth (DOB)
- Mailing Address

- Zip Code
- Phone Number(s)
- Email Address
- Eligibility Status
- Next of Kin (NOK) Information
- Veteran Call History
- Integrated Control Number (ICN)

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.

Whenever technically feasible, all records are retained for two years – in case additional follow-up actions on behalf of the individual become necessary. However, any documents the Veteran wants removed from the system will be purged from the system upon request via the Amendment of Records process.

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.

Information retention for the Call Centers is maintained for two years. All records are retained for a period of two years in case additional follow-up actions on behalf of the individual become necessary. Data is stored in the Microsoft - Azure Government (includes Dynamics 365) cloud. Application location information is as follows:

Application Component	Name	Location Which Component is From	Type
ECC CRM	Main Facility	For security reasons, Microsoft does not provide a Physical address for its data centers. However, redundant Microsoft Government cloud regions exist inboth Boydton, Virginia and Des Moines, Iowa	Production Host: Application and Data Store
ECC CRM	Default Failover Facility	For security reasons, Microsoft does not provide a Physical address for its data centers. However, redundant Microsoft Government cloud regions exist inboth Boydton, Virginia and Des Moines, Iowa	Production Host: Application and Data Store

A Backup Plan and Restore Plan is developed and implemented for the cloud-hosted environment using Dynamics 365 native Backup/restore capabilities (see https://docs.microsoft.com/enus/ dynamics365/customer-engagement/admin/backup-restore-instances) and industry best practices. At a minimum, the plan shall include the requirement to save data for the backup and recovery of information stored on the cloud storage infrastructure to meeting related Standard Level Agreements (SLAs) and the retention of records as required by VA Handbook 6300.1 (Records Management Procedures) and VA Directive 6300 (Records and Information Management). CRM production data is retained for 14 days and restored to each application's production environment per request. Backups are conducted on a daily basis and as needed per application team request.

The Federal Records Act of 1950, as amended, contains the statutory authority for VBA records management. Government-wide responsibility for Federal recordkeeping is shared by the General Services Administration (GSA) and NARA. Title 44 of the United States Code (U.S.C.) §§ 3301 through 3314 establishes the legal basis for the disposal of records of the United States Government. All electronic permanent records and VA sensitive information records are treated the same as hardcopy records and should follow an approved record disposition plan, see VBA RCS (VB-1)(VB-2), to include; (1) retaining, (2) transferring to a records center for temporary storage, (3) transferring to an archival agency, (4) donating to an eligible repository, and (5) transferring to an approved image reproduction vendor.

NOTE: Never delete permanent records or VA sensitive information.

It is VBA policy that all Federal records contained on paper, electronic, or other media are properly managed from creation through final disposition, in accordance with federal laws, the General Records Schedule (GRS) and VBA Records Control Schedule (VBA RCS) (VB-1)(VB-2). VBA is committed to enforcing the proper disposition of Veterans' records by ensuring the records are appropriately protected and maintained. The Records Management Officer (RMO), Records Management Technician (RMT), and supervisors will work together to ensure all VBA employees and affected parties follow established procedures for storing, routing, and disposing of Veterans' paper and electronic records.

POLICIES AND PRACTICES FOR STORING, RETRIEVING, ACCESSING, RETAINING, AND DISPOSING OF RECORDS IN THE SYSTEM:

Paper documents received (such as DD214 forms, letters, emails, applications, verification of employment or any education related documents) are scanned into VA's electronic document repository (The Image Management System (TIMS)) and subsequently destroyed after 90 days. Electronic records are not purged.

3.4 What are the procedures for the elimination of SPI?

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

The ECC CRM application will follow NIST 800-88 ("Guidelines for Media Sanitization") to destroy data as part of the decommissioning process of any IT storage hardware used in the ECC CRM application. The Guidelines establish three levels of data destruction: Clear, Purge, and Destroy, that can be applied to different data storage devices. An appropriate destruction method will be chosen based on the memory type (Flash Memory, Magnetic Drives, Optical Devices, Hard Copies etc.) used for the storage. It is VA policy that all Federal records contained on paper, electronic, or other medium are properly managed from their creation through their final disposition, in accordance with Federal laws, the General Records Schedule and the VBA Records Control Schedule VBA RCS (VB-1)(VB-2). It provides a brief description of the records and states the retention period and disposition requirements. It also provides the NARA disposition authorities or the GRS authorities, whichever is appropriate for the records, in addition to program and service sections.

In regards to temporary paper records, in particular those that contain PII, and VA sensitive information, which are under the jurisdiction of VA, will be handled securely, economically, and effectively and disposed of properly. Written documentation that attests to the completion of the destruction process after the final destruction is required, which could be in the form of a letter, memo, or any format attesting to its complete destruction. This certification is not considered a valid certification of destruction if completed and submitted prior to the final destruction of the records. The certification should contain sufficient information to attest to the final destruction of the temporary paper records – what temporary records were destroyed, the date when they were destroyed, what destruction method was used, where they were destroyed, and who was responsible for their final destruction. (VA Directive 6371, 04/08/2014).

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

PII is not used during testing or training. Test Veterans with artificial data are used to test the application. Test Veterans are provided by DGI and BDN. End-users utilize the same test Veterans during training. Additionally, all training materials display example data using test Veterans. At this time, ECC CRM data is not used for Research. The project team plans to de-identify all data to minimize the risk to privacy when using PII for research.

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: The risk to maintaining data within the ECC CRM application for a longer time period than what is needed or required is that the longer information is kept, the greater the risk that information will be compromised, unintentionally released, or breached.

Mitigation: The ECC CRM application retains information for a period of two years for its purpose of helping the Veteran and their dependents with their questions regarding their education benefits, and management of information of the call activity. PII outlined in Section 3.1 and, the reason of call and resolution provided is retained by the ECC CRM application, as the system of record for phone interactions. This information gives management the ability to report on types of calls, first call resolution, and time to solve Veteran issues.

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.

The Customer Service Representatives (CSR) goes through trainings required by the VA to access the PII. Each of the CSRs need credentials from the VA systems integrated with the ECC CRM application and has to follow process, and procedures required by those VA systems. Only the trained users approved by the ECC CRM Management or VA IT can obtain credentials to access the ECC CRM application.

The ECC CRM application does not internally share any data that is being held in the system. The ECC CRM application does receive information from other VA systems which are listed in the Table 3 below, along with the type of the information received and its use.

The Call History data is retained in CRM and is used to assist a seasoned CSR if a call is escalated, to provide consistency in responses for callers who call multiple days and for reporting purposes by ECC CRM Management.

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***
Benefits Delivery Network (BDN)	Needed to obtain Payment, Debt and Beneficiary Profile	Payment, Debt, and Beneficiary Profile Information	Encrypted electronic transmission

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***
	Information required to confirm a Veteran caller's identity. Information is received from the system, not shared with the system		
Flight, On-the-Job Training, Correspondence and Apprenticeship System (FOCAS)	Needed to obtain Enrollment Information for On-the-Job Training Programs required to assist a Veteran caller. Information is received from the system, not shared with the system	Enrollment Information for On-the-Job Training Programs	Encrypted electronic transmission
Digital GI Bill (DGI) *Formerly Long Term Solution (LTS)*	Needed to obtain Benefits Enrollment, Payment, Debt, and Beneficiary Profile Information required to confirm a Veteran caller's identity. Information is received from the system, not shared with the system	Benefits Enrollment, Payment, Debt, and Beneficiary Profile Information	Encrypted electronic transmission
SHARE (Microsoft Application)	Needed to obtain Payment and Beneficiary Profile information required to assist a Veteran caller. Information is received from the system, not shared with the system	Payment and Beneficiary Profile Information	Encrypted electronic transmission
The Image Management System (TIMS)	Request for Information to the regional processing office regarding a caller's case in order to assist Veteran caller	ECC CRM coordinates with VA Regional Processing Offices via TIMS to get updates in case processing	Encrypted electronic transmission
Veteran Information Solution revised (VISr)	Needed to obtain Beneficiary Profile Information required to assist Veteran caller. Information is received from the system, not shared with the system	Beneficiary Profile Information	Encrypted electronic transmission

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*
Web Enabled Approval Management System (WEAMS)	Needed to obtain facility and School Certifying Official (SCO) information required to assist Veteran caller. Information is received from the system, not shared with the system	Facility and School Certifying Official (SCO) information	Encrypted electronic transmission
Performance Analysis and Integrity (PA&I)	Needed to obtain Beneficiary Profile Information and return of system identifiers. Information is received from the system, not shared with the system	Beneficiary Profile Information	Encrypted 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 ECC application does not share any data that is being held in the system. The ECC application receives information from MPI, BDN, DGI, WEAMS, VIS-r, FOCAS and TIMS. Users can copy the information received in the system and disseminate information to unauthorized.

Mitigation: Information is presented to help the CSRs answer caller's question. The information received from the VA systems identified above is encrypted during transmission and is not stored in the CRM. ECC application users are not allowed to carry PII information outside of the call center premises.The print buttons are disabled for VIS-r, and Service Requests created to prohibit creating of hard copies of the information received via the application. Users are also required to go through the privacy trainings and are trained in handling PII before they are given access to the ECC application.

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***
N/A	N/A	N/A	N/A	N/A

ECC CRM does not share any data that is being held in our system.

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 ECC application does not share any data that is being held in the system. Therefore, no privacy risks are associated with sharing information outside of the VA. The system tracks access made to the ECC application, and changes made to the information stored in the CRM system. The ECC application only accesses education benefit, and payment information of the beneficiaries. Such information if disclosed intentionally or unintentionally will negatively impact the more than 10,000 callers and VA VBA reputation, and the trust beneficiary provided to the VBA. The PII information if gone to the wrong hands can be used for identify theft.

Mitigation: Only trained VA employees approved by the ECC, or IT support personnel's approved by the VA IT have access to the ECC application.

Section 6. Notice

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

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

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

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

Describe how the notice provided for the collection of information is adequate to inform those affected by the system that their information has been collected and is being used appropriately. Provide information on any notice provided on forms or on Web sites associated with the collection.

This question is related to privacy control TR-1, Privacy Notice, and TR-2, System of Records Notices and Privacy Act Statements, and TR-3, Dissemination of Privacy Program Information.

The ECC application is not a system of record of VA education program beneficiary or their benefits, and also does not collect beneficiary medical information. The ECC application logs the beneficiary that contacted the call center, the reasons for their contact and how the call center supported the caller. As PII including SSN can be saved to group the interaction made between the caller and call center by benefits recipient, these types of records have been covered under the Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records—VA (58VA21/22/ 28) SORN. The VA policy is not to disclose any personal information to third parties outside VA without their consent, except to facilitate the transaction, to act on caller's behalf at their request, or as authorized by law. Any questions or concerns regarding VA privacy policy or use of caller's information can be made by contacting via email at Contact VA Privacy Service, or by mailing questions or concerns at Department of Veterans Affairs, Privacy Service, 810 Vermont Avenue, N.W. (005R1A) Washington, DC 20420.This Privacy Impact Assessment will be available online as required by the eGovernment Act of 2002, Pub.L. 107–347§208(b)(1)(B)(iii). More detail on privacy policy that ECC is required to follow can be found at VA Privacy Policy. Posted privacy policy, Privacy Act statements are published via SORN in the Federal Register https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24372.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

Veterans have the right to refuse to disclose their SSNs to VBA. The individual shall not be denied any right, benefit, or privilege provided by law because of refusal to disclose to VBA an SSN (please refer to the 38 Code of Federal Regulations CFR 1.575(a)).

Depending on the nature of the program or information system, it may be appropriate to allow individuals to limit the types of PII they provide and subsequent uses of that PII. VA consent mechanisms include a discussion of the consequences to individuals for failure to provide PII.

Additionally, the Compensation, Pension, Education and Vocational Rehabilitation and Employment Records – VA (58VA21/22/28) SORN provides individuals their rights regarding opportunities to decline to provide information.

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

All requests must be in writing and adequately describe the specific information the individual believes to be inaccurate, incomplete, irrelevant, or untimely and the reason for this belief. The written request needs to be mailed or delivered to the VBA address outlined within the Compensation, Pension, Education and Vocational Rehabilitation and Employment Records – VA (58VA21/22/28) SORN.

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 Veterans who provide information to the ECC application, as mentioned above, will not know how their information is being stored.

Mitigation: The VA mitigates this risk by providing the public with one form of notice that the ECC application exists through the Privacy Impact Assessment (PIA) which is posted for public access.

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.

Veterans may request access to Privacy Act records maintained by requesting a copy in writing. All requests to review must be received by direct mail, fax, in person, or by mail referral from another agency or VA office. All requests for access must be delivered to, and reviewed by the System Manager for the concerned VBA system of records, the facility Privacy Officer, or their designee. Each request must be date stamped and reviewed to determine whether the request for access should be granted.

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.

Veterans have the right to amend their records by submitting their request in writing. The request must be in writing and adequately describe the specific information the individual believes to be inaccurate, incomplete, irrelevant, or untimely and the reason for this belief. The written request needs to be mailed or delivered to the VA Regional Office that maintains the record. A request for amendment of information contained in a system of records must be delivered to the System Manager, or designee, for the concerned VBA system of records, and the facility Privacy Officer, or designee, and needs to be date stamped; and filed appropriately. In reviewing requests to amend or correct records, the System Manager must be guided by the criteria set forth in VA regulation 38 CFR 1.579.

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.

In case the information in the ECC application is inaccurate, Veterans have the right to request amendment of erroneous information in accordance with the Privacy Act. Individuals have the right to request an amendment (or correction) to information in the ECC records if they believe it is incomplete, inaccurate, untimely, or unrelated to their education benefits. ECC does not address any health information records with their callers. Calls of this nature are transferred to the National Call Center. The individual must submit the request in writing, specify the information that should be corrected, and provide a reason to support the request for amendment. All amendment requests should be submitted to the facility Privacy Officer at the VBA facility that maintains your information. In response, the individual may do any of the following:

- File a "Statement of Disagreement".
- Ask that your initial request for amendment accompany all future disclosures of the disputed information.

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.

Formal redress is provided in SORN. All information correction must be taken via the Amendment process. In addition, the individual may contact any Regional Office for guidance on how to gain access to his or her records and seek corrective action through the Amendment 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: There is a risk that incorrect information is accidentally recorded in an individual's record. An individual may want to review the content of their record to check for data accuracy.

Mitigation: Veterans have the right to amend their records by submitting their request in writing. The request must be in writing and adequately describe the specific information that individual believes to be inaccurate, incomplete, irrelevant, or untimely and the reason for this belief. The written request needs to be mailed or delivered to the VA Regional Office that maintains the records. A request for amendment of information contained in a system of records must be delivered to the System Manager or designee for the concerned VBA system of records, and the facility Privacy Officer or designee, and needs to be date stamped; and filed appropriately. In reviewing request to amend or correct records, the System Manager must be guided by the criteria set forth in VA regulation 38 CFR 1.579.

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.

The Office of Information and Technology (OIT) documents and monitors individual information system security training activities, including basic security awareness training and specific information system security training. This documentation and monitoring is performed through the use of Talent Management System (TMS). Access to the system is granted to VA employees and contractors by the local authority within each administrative area staff office, following the described account creation process. Only the IT system admins authorized by VA IT will have the security role to modify the ECC

application. There are three types of users who use the system on a daily basis: CSRs, senior CSRs, and supervisors. Most of the users using the system are CSRs and senior CSRs, and they can only create files in the system and have limited access to data. Limited users from the call center have supervisor security role granted in the CRM system for the purpose of creating call center reports. The users with only ECC application credentials cannot access education program beneficiary information. They will need to apply for credentials separately with each of the systems integrated in the ECC application.

Developer Access

Developers account management processes should further ensure that only end-users are able to access the environment. Developers and ECC Project teams will work to create, update, access and disable developer accounts for project teams. Additionally, there shall be a review of user access periodically to evaluate whether users are active in the environment; if the user is not active, their account is terminated. A designated VA Project POC is the only person who may submit account creation requests and submitted for accountability purposes.

End-User and Tester Access

All individuals requesting developer access are required to complete all VA trainings (VA Privacy and InformationSecurity Awareness and Rules of Behavior Training, Privacy and HIPAA Focused Training and Information Security for IT Specialists Training), and must be authorized by VA Project Manager. To ensure that this requirement is met, the designated VA Project POC must submit a signed Access Request Form for an individual or a group. At minimum, the following information should be provided for each VA Project Team member requesting access to the ECC application Environments: First Name, Last Name, Primary E-mail, Main Phone, Manager, Current on VA Training, VA Employee or Contractor, VA Active Directory Username, Environment, Access Permissions, and Contract End date.

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 have access to the pre-production environments for development purposes. Contractors are bound by the same privacy and security procedures and requirements as VA employees. Contractors also have access to the live production system for maintenance activities. The following steps are required before contractors can gain access to the system:

- Contractors must take and pass training on VA Privacy and Information Security Awareness and Rules of Behavior (VA 10176) and Privacy and HIPAA Training (VA 10203), and government ethics and role-based training based on support role to the system.

- Contractors must have signed the Non-Disclosure Agreement (NDA) and Rules of Behavior (RoB).
- Contractors must have successfully completed VA contractor background security investigation as per the Position Designation Automated Tool (PDT).
- Once complete, a request is submitted for access. Before access is granted to the production environment; this request must be approved by the supervisor, and OIT.

VA owns the data that the ECC application extracts from the source applications, and Microsoft manages and secures the ECC application data. The VA and Microsoft Project Managers, CORs have weekly meetings for the review of the contract details and this contract is reviewed at least on anannual basis.

There shall be a regular review of user access to evaluate whether users are active in the environment. If a user is not active, the account will be terminated. A designated VA Project POC is the only person whomay submit account creation requests for accountability purposes. Contractor access to the system expires at the end of the contract duration or earlier.

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 who will be accessing information systems must read and acknowledge their receipt and acceptance of the VA 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 mustcomplete via the VA's Talent Management System (TMS). After the ECC user's initial acceptance of the Rules, the user must re-affirm their acceptance annually as part of the security awareness training. Acceptance obtained through electronic acknowledgment is tracked through the TMS system. All VA employees must complete annualPrivacy and Security training. This training includes, but is not limited to, the following TMS Courses:

- VA 10176: Privacy and Info Security Awareness and Rules of Behavior
- VA 10203: Privacy and HIPAA Training
- VA 3812493: Annual Government Ethics
- Role-based Training Includes, but is not limited to and based on the role of the user:
- VA 1016925: Information Assurance for Software Developers IT Software Developers
- VA 3193: Information Security for Chief Information Officers (CIOs) Executives, Senior
- Managers, CIOs and Chief Financial Officers (CFOs)
- VA 1357084: Information Security Role-Based Training for Data Managers
- VA 64899: Information Security Role-Based Training for IT Project Managers
- VA 3197: Information Security Role-Based Training for IT Specialists
- VA 1357083: Information Security Role-Based Training for Network Administrators
- VA 1357076: Information Security Role-Based Training for System Administrators

- VA 3867207: Information Security Role-Based Training for System Owners

ECC users agree to comply with all terms and conditions of the National Rules of Behavior, by signing acertificate of training at the end of the training session.

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

If Yes, provide:

1. *The Security Plan Status, Approved*
2. *The Security Plan Status Date, 9/24/21*
3. *The Authorization Status, Authorization to Operate*
4. *The Authorization Date, 6/10/2022*
5. *The Authorization Termination Date, 12/7/2022*
6. *The Risk Review Completion Date, 6/10/2022*
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH). MODERATE*

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

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

There are two components necessary for the ECC application to operate. They are as follows:

1. Application ATO: The ECC application is covered under the "BAM CRM Moderate Assessing"ATO which was approved on January 3, 2022 and expires on July 2, 2022.
2. Cloud Hosting ATO: The ECC application is hosted on the Microsoft – Azure Government (includes Dynamics 365). The "Microsoft – Azure Government Assessing" ATO was approved on February 27, 2020 and expires on February 26, 2023.

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 Cloud Service Provider for ECC CRM is Microsoft - Azure Government (includes Dynamics 365).

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.

Yes, VA has full ownership of the PII that will be shared through the ECC CRM platform, as established under the Microsoft Dynamics 365 Cloud Services Contract, Contract Number: 47QTCA22D003G-36C10B22F0089.

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.

No ancillary data is collected by this application.

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

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

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

The Contractor/Subcontractor must store, transport, or transmit VA sensitive information in an encrypted form, using VA-approved encryption tools that meet Federal Information Processing Standards.

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 use RPAs or "bots" are not implemented within the ECC CRM application.

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.

BERTHA BROWN Digitally signed by BERTHA BROWN
Date: 2022.06.24 15:07:28 -04'00'

Privacy Officer, Bertha. L. Brown

Thomas J. Orler 178546 Digitally signed by Thomas J. Orler 178546
Date: 2022.06.26 11:55:53 -05'00'

Information System Security Officer, Thomas Orler

Stefano Masi 474380 Digitally signed by Stefano Masi 474380
Date: 2022.06.27 07:02:48 -04'00'

Information System Owner, Stefano Masi

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).

Compensation, Pension, Education, and Rehabilitation Records –VA (58VA21/22/28)

https://www.oprm.va.gov/docs/Current_SORN_List_2_25_2022.pdf