Privacy Impact Assessment for the VA IT System called:

Visitor Outreach, Interaction, and Communication Engine (VOICE)

Veterans Benefits Administration (VBA)

Veteran Relationship Management (VRM)

eMASS ID 2520

Date PIA submitted for review:

11/4/2024

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Marvis Harvey	Marvis.Harvey@va.gov	202-461-8401
Information System Security Officer (ISSO)	Albert Estacio	Albert.Estacio@va.gov	909-583-6309
Information System Owner	Izel Cruz Maisonave	Izel.CruzMaisonave@va.gov	202-632-8202

Abstract

The abstract provides the simplest explanation for "what does the system do for VA?".

Customer Relationship Management (CRM) - Visitor Outreach, Interaction, and Communication Engine (VOICE) will be used by authorized contact representatives. It will provide CRM services based on the Microsoft Dynamics CRM Product to National Call Centers (NCCs) and multiple Regional Offices (ROs) that respond to calls related to services provided by the Veterans Benefit Administration (VBA). This will be the modernized version of the current Customer Relationship Management – Unified Desktop Optimization (CMR UD-O). VA Solid Start (VASS) will be part of VOICE. VASS enables call center agents and administrators to make outbound calls to recently transitioned service members, regardless of the character of discharge, at key intervals during the first year after separation from military service, in response to Executive Order (EO) 13822.

Overview

The overview is the most important section of the Privacy Impact Assessment (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:

1 General Description

A. What is the business purpose of the program, IT system, or technology and how it relates to the program office and agency mission?
CRM VOICE is the modernized version of CRM UD-O, which facilitates a modern, customer-centric experience for VA call center agents, enabling them to efficiently gather benefit information for Veterans, their beneficiaries, and authorized representatives. CRM VOICE endeavors to furnish them with seamless and convenient interactions when engaging with the VA across various communication channels at the National Call Centers (NCCs) and Public Contact Teams (PCTs), including recently transitioned service members through the VA Solid Start (VASS) program, and PACT Act eligible Veterans.

B. Who is the owner or has control of the IT system or project? If the system has an eMASS entry, ensure this information matches with the eMASS entry.
VA Owned and VA Operated

2. Information Collection and Sharing

Indicate the expected number of individuals whose information is stored in the system and include a brief description of the typical client or affected individual?

Over one million (1,000,000) veterans and beneficiaries are served, it provides information to support them and their dependents accurately regarding VA's benefits and resources.

Check if Applicable	Demographic of individuals
☒	Veterans or Dependents
☐	VA Employees
☐	Clinical Trainees
☐	VA Contractors
☐	Members of the Public/Individuals
☐	Volunteers

C. What is a general description of the information in the IT system and the purpose for collecting this information?

CRM VOICE collects and processes PII/PHI and other beneficiary information to assist in processing support for Veterans and Beneficiaries. It interfaces with multiple legacy VA benefit systems to provide a detailed overview of each Veteran's benefit information and history. It also provides information to VA Solid Start (VASS) agents to assist recently transitioned service members.

D. What information sharing is conducted by the IT system? A general description of the modules and components, where relevant, and their functions.

VA agents at the National Call Centers (NCCs) and Public Contact Teams (PCTs) will access comprehensive veteran profiles and interactions, enabling personalized and efficient responses to support our Veterans, their beneficiaries, and representatives with quick, correct and timely information about their earned benefits and services. It interfaces with multiple legacy VA benefit systems to provide a detailed overview of each Veteran's benefit information and history. It will use the add-in chat feature to interact with VASS users. It also allows for note taking and Veteran interaction history, allowing VA agents to provide accurate and timely responses to our Veterans. Benefits information is displayed through the browser using Customer Service Workspace (CSW) instead of the Unified Service Desk (USD), which was used in CRM UD-O. CRM VOICE provides upgrades and enhancements to the existing Microsoft CRM software originally developed and implemented by the CMR UDO/Knowledge Management (KM) project under the Veterans Relationship Management (VRM).

E. Are the modules/subsystems only applicable if information is shared?

No information is shared outside the VA.

F. Is the system operated in more than one site to include primary and secondary 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?

Call center agents use the CRM VOICE at the VA National Call Centers (NCCs) to facilitate easier and more efficient interactions with Veterans and their beneficiaries.

3. Legal Authority and System of Record Notices (SORN)

G. What is the citation of the legal authority and SORN to operate the IT system?

58VA21/22/28 Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA" (11/8/2021) https://www.govinfo.gov/content/pkg/FR-2021- 11-08/pdf/2021-24372.pdf (2) 57VA10 Voluntary Service Records-VA (11/08/2021)

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: Title 10 U.S.C. chapters 106a, 510, 1606 and 1607 and title 38, U.S.C. §501(a) and Chapters 3, 11, 13, 15, 18, 19, 21, 23, 30, 31, 32, 33, 34, 35, 36, 37, 39, 51, 53, 55 and 77. Title 5 U.S.C. 5514. 2021-24372.pdf (govinfo.gov)

H. What is the SORN?

58VA21/22/28 Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA" (11/8/2021)
57VA10 Voluntary Service Records-VA (11/08/2021) https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24372.pdf

I. SORN revisions/modification

The system of record notices does not require modifications.

I. If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval.

The system of record notices does not require amendments.

4. System Changes

J. Will the business processes change due to the information collection and sharing?

☐ *Yes*
☒ *No*
if yes, <<ADD ANSWER HERE>>

K. Will the technology changes impact information collection and sharing?

☐ *Yes*
☒ *No*

if yes, <<ADD ANSWER HERE>>

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 Information 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. It must also match the information provided in question 3.4 of the PTA.

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
- ☒ **Full** Social Security Number
- ☐ **Partial** 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 Information
- ☐ Health Insurance Beneficiary Numbers Account Numbers
- ☐ Certificate/License numbers[1]
- ☐ Vehicle License Plate Number
- ☐ Internet Protocol (IP) Address Numbers
- ☐ Medications
- ☐ Medical Records
- ☐ Race/Ethnicity
- ☐ Tax Identification Number
- ☐ Medical Record Number
- ☒ Gender/Sex
- ☒ Integrated Control Number (ICN)
- ☒ Military History/Service Connection
- ☒ Next of Kin
- ☒ Date of Death
- ☐ Business Email Address
- ☒ Electronic Data Interchange Personal Identifier (EDIPI) ☒ Other Data Elements (list below)

[1] *Specify type of Certificate or License Number (e.g., Occupational, Education, Medical)

Other PII/PHI data elements:

- Veteran benefits payments, Veteran ratings, awards, insurance information, health information and payments
- Demographics (includes Gender and Date of Death)
- Contact History (e.g. Payment details, demographics, addresses)
- Exam Appointment Information
- Release from Active-Duty Date
- Username

1.2 List the sources of the information in the system

These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

1.2a 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?

The information comes from the Veteran or from systems already storing Veteran information: Beneficiary Identification and Records Locater Subsystem (BIRLS), Modern Award Processing Development (MAP-D), SHARE, Veterans Service Network (VETSNET), BEP, VIERS, VA Profile, Compensation and Pension Records Interchange (CAPRI), Finance and Accounting Services (FAS), CORP DB (Corporate Database). Consolidated Mail Outpatient Pharmacy (CMOP).

1.2b 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 indicate why the system is using this source of data.

No information is required from additional sources or aggregators.

1.2c Does the system create information (for example, a score, analysis, or report), list the system as a source of information?

*No, t*he information comes from the Veteran or from systems already storing Veteran information.

1.3 Methods of information collection

These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

1.3a 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 technologies used in the storage or transmission of information in identifiable form?

The National Call Center (NCC) will use CRM VOICE, in some cases data will be collected using interfaces with other backend systems, and in other cases data will be collected by VA employees using webforms as they interact with callers.

1.3b If the information is collected on a form and is subject to the Paperwork Reduction Act, what is the form's OMB control number and the agency form number?

No information will be collected on forms and will not be subject to the Paperwork Reduction Act.

1.4 Information checks for accuracy, and how often will it be checked.

These questions are related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.

1.4a 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.

The information that will be collected will be used to identify Veterans and to assist the NCC agents with delivering accurate and efficient service to each caller. By storing basic information, including demographic data, an agent can quickly identify who is calling and what they can do to solve their inquiries. Information typed and stored directly in the CRM tool is vetted by the NCC agents who ask Veterans to verify the information that they see (and collect) and along with information that is pulled and displayed from various legacy VA backend systems.

1.4b Does the system check for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract?

No commercial aggregator is used.

1.5 Identify the specific legal authorities, arrangements, and agreements that 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-Veterans' Benefits, Joint Commission National Patient Safety Goals- Goal 1: Improve the accuracy of patient identification, Office of Management and Budget (OMB) Circular A-130, Management of Federal Information Resources, Appendix III, November 2000

System of Record Notice, 58VA21/22/28 Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA" (11/8/2021)
https://www.govinfo.gov/content/pkg/FR-2021-11 08/pdf/2021-24372.pdf
(2) 57VA10, Voluntary Service Records VA (1/25/2023)

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. (*Work with your System ISSO to complete this section)*

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

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

Principle of Minimization: The information is directly relevant and necessary to accomplish the specific purposes of the program.

Principle of Individual Participation: The program, to the extent possible and practical, collects information directly from the individual.

Principle of Data Quality and Integrity: VA policies and procedures must ensure that personally identifiable information is accurate, complete, and current.
This 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: Where application collect Personally Identifiable Information (PII), if this information were released to inappropriate parties or the public, it could result in financial, personal, and/or emotional harm to those individuals.

Mitigation: Application mitigates the risk of identity theft by requiring all applicable Contractors and VA employees who engage with CRM VOICE to complete all the following data security and privacy 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 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 that 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.

PII/PHI Data Element	Internal Use	External Use
Name	Veteran's identification	Not used
Gender/Sex	Used to verify Veteran identity	No used
Social Security Number	Used to verify Veteran identity and as a file number for Veteran	Not used
Date of Birth	Used to verify Veteran identity	Not used
Mailing Address	Used to correspond with the Veteran	Not used
Zip Code	Part of the mailing address	Not used
Phone Number(s)	Used to correspond with the Veteran	Not used
Email Address	Used to correspond with the Veteran	Not used
Emergency Contact Information (Name, Phone Number, etc. of a different individual)	Used in emergencies to contact the Veteran	Not used
Eligibility Status	Used to provide relevant information on entitlement	Not used
Next of Kin (NOK) Information	Used in emergency to contact the Veteran	Not used
Veteran Call History	Used to provide call development and resolution data	Not used
ICN	Used to identify veterans and beneficiary records between system	Not used
Financial Information	Payments Banking Direct Deposit	Not used
Military History/ Service Connection	Eligibility and Benefits determination Targeted outreach to Veterans in support of initiatives Administration and delivery	Not used
Demographics	Used to view Veteran's Date of Death, Gender	Not used

2.2 Describe the types of tools used to analyze data and what type of data may be produced.
These questions are related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information.

2.2a 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?

In general, the information that will be stored in CRM VOICE are various management, tracking, and follow-up reports that are used to assist in the management and operation of the National Call Center (NCC). Microsoft CRM has internal tools to generate graphs and reports of specific data.

2.2b 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.

VOICE does not create any new information as all new collected data (Dependent Changes, FNOD, ITF, etc.), for which VOICE is not the SOR, is immediately passed to the appropriate SOR. All data generated data by VOICE (Notes, Interaction History) for which VOICE is the SOR will be stored in VOICE and uploaded to the CxW Data Lake. VOICE will be SOR for Security PIN but will not be shared.

2.3 How the information in the system is secured.

These questions are related to security and privacy controls SC-9, Transmission Confidentiality, and SC-28, Protection of Information at Rest.

2.3a What measures are in place to protect data in transit and at rest?

Data within the VA network is FIPS 2.0 encrypted.

2.3b If the system is collecting, processing, or retaining Social Security Numbers, are there additional protections in place to protect SSNs? (refer to PTA question 3.8).

Access to system is limited, requires PIV; and access to system and components are audited in accordance with VA 6500. The information received from the VA systems identified are encrypted during transmission, and all data is encrypted during communication from a call agent's desktop to all VA endpoints.

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

Contractor and VA employees are required to take Privacy, HIPAA, and information security training annually. HTTPS using SSL encryption is used between internal VA systems. 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. VEIS uses HTTPS, TLS, oAuth tokens and OSP APIM for additional encryption. Connections to VEIS endpoints are encrypted and authenticated using TLS 1.3, P-384, and AES_256_GCM.

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information.

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.

2.4a How is access to the PII determined?

Yes, the PIA and SORN are applicable and clear about how the information collected on each Veteran is used. The mission of the project is to deliver exceptional customer service to the Veterans and the information stored in the system is used to create a record of a Veteran to ensure timely and accurate assistance is given. Access is determined by the program and upon approval, it is the responsibility of the project making the request to ensure compliance with VA regulations and policies regarding configurations, privacy restrictions, network access and authorities or operates (including but not limited to: VA 6500, TIC, PIA/PTAs, SORN, and application ATOs). Needed access / Approved submitters request access with the needed roles.

2.4b Are criteria, procedures, controls, and responsibilities regarding access documented? How are the documented, i.e. Policy, SOP, other. And where is this documentation located?

Yes, criteria, procedures, controls, and responsibilities are documented and also available for VA employees in the KM - Knowledge Management site.

2.4c Does access require manager approval?

Yes, access requires manager approval.

2.4d Is access to the PII being monitored, tracked, or recorded?

Yes, it is the responsibility of the project making the request to ensure compliance with VA regulations and policies regarding configurations, privacy restrictions, network access and authorities or operates. (Including but not limited to: VA 6500, TIC, PIA/PTAs, SORN, and application ATOs).

2.4e Who is responsible for assuring safeguards for the PII as identified in eMASS?

It is the responsibility of the project making the request to ensure compliance with VA regulations and policies regarding configurations, privacy restrictions, network access and authorities or operates (including but not limited to: VA 6500, TIC, PIA/PTAs, SORN, and application ATOs).

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
- Full Social Security Numbers
- Date of Birth
- Personal Mailing Address
- Personal Phone Number
- Personal Email Address
- Emergency Contact
- Financial Information
- Gender/Sex
- Integrated Control Number (ICN)
- Military History/Service
- Date of Death
- Electronic Data Interchange Personal Identifier (EDIPI)
- Veteran benefits payments, Veteran ratings, awards, insurance information, health information and payments
- Demographics (includes Gender and Date of Death)
- Contact History (e.g. Payment details, demographics, addresses)
- Exam Appointment Information
- Release from Active-Duty Date
- Username

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.*** *If the system is using cloud technology, will it be following the NARA approved retention length and schedule https://www.archives.gov/records-mgmt/grs? This question is related to privacy control DM-2, Data Retention and Disposal.*

Records Control Schedule: General Records Schedule (GRS) 6.5 *Public Customer Service Records*.

Section: Nothing is applicable – it uses other application data for viewing purposes only.

Retention/Disposition: Information is retained for one year.

Information is retained for one year, in accordance with GRS 6.5 Item 010.

3.3 The retention schedule approved by the VA records office and the National Archives and Records Administration (NARA).

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. Please work with the system VA Records Officer to answer these questions.
This question is related to privacy control DM-2, Data Retention and Disposal.

3.3a Are all records stored within the system of record indicated on an approved disposition authority?

Yes, records are stored in the Records Control Schedule (RCS) 10-1
https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf

OI&T GRS 005-1.
https://www.archives.gov/files/records-mgmt/grs/grs06-5.pdf (GRS 6.5)

3.3b Please indicate each records retention schedule, series, and disposition authority?

Yes, follows GRS 6.5 Item 010. https://www.archives.gov/files/records-mgmt/grs/grs06-5.pdf (GRS 6.5)
AA-GRS2017-0002- 0001

3.4 What are the procedures for the elimination or transfer of SPI?

Explain how records are destroyed, eliminated, or transferred to NARA at the end of their mandatory 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.

Electronic data and files of any type, including PHI, SPI, Human Resources records, and more are destroyed in accordance with the Media Sanitization section of the VA Directive 6500 VA Cybersecurity Program (February 24, 2021) and are compliant with NIST SP 800-88. 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. Digital media is shredded or sent out for destruction.

https://www.va.gov/vapubs/search_action.cfm?dType=1.

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. This question is related to privacy control DM-3, Minimization of PII Used in Testing, Training and Research.

Only approved for testing SSNs (fake Veterans) are used when testing by those not cleared to access or view live Veteran data. This limits PII to only those who need to see it and can do so, based on their job duties. No data is used for research, testing, or training. Per OBI, no fake use of SSNs should be used in production.

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. (Work with your System Privacy Officer (PO) to complete all Privacy Risk questions inside the document this section).

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: The project retains only the information necessary for its purpose, additionally, the PII is retained only for as long as necessary and relevant to fulfill the specified purposes.

Principle of Data Quality and Integrity: The PIA should describe 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 maintained by CRM VOICE may be retained for longer than necessary to fulfill the VA mission. Records held longer than required are at greater risk of being unintentionally released or breached.

Mitigation: To mitigate the risks of information retention, CRM VOICE will adhere to NARA Records Control Schedule. When a records retention date is reached, the individuals' information is disposed of by the method described in RCS 10. Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

The following questions are intended to define the scope of information sharing/receiving/transmitting within VA.

PII Mapping of Components

4.1a CRM VOICE consists of 8 key components (servers/databases/instances/applications/software/application programming interfaces (API)). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by CRM VOICE and the reasons for the collection of the PII are in the table below.

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

Internal Components Table

Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI	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
	Yes	Yes	Social Security Number	ID Proof	This application is within VA and has FIPS

Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI	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
Financial and Accounting Systems (FAS)					2.0 encryption.
Corporate Database	Yes	Yes	Social Security Number, Address, Telephone Number, Email Address	ID Proof	This application is within VA and has FIPS 2.0 encryption.
EFolder	Yes	Yes	Customer Name, SSN	Virtual Documentation	This application is within VA and has FIPS 2.0 encryption.
IAM- Master Person Index (IAMMVI)	Yes	Yes	First Name, Last Name, SSN	ID Proof	This application is within VA and has FIPS 2.0 encryption.
Benefits Enterprise Platform (BEP)	Yes	Yes	Contact History (e.g. Payment details, demographics, addresses)	ID Proof	This application is within VA and has FIPS 2.0 encryption.
Veteran Identity/Eligibility	Yes	Yes	Name, SSN, DOB,	ID Proof	This application is within VA

Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI	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
Reporting Systems (VIERS)			(EDIPI), User Names		and has FIPS 2.0 encryption.
Health Data Repository (HDR)	Yes	Yes	Names, SSN, Exam Appointment Information	ID Proof	This application is within VA and has FIPS 2.0 encryption. This application is within VA and has FIPS 2.0 encryption.
VA Profile	Yes	Yes	Address, Telephone Number, Email Address, Active Prescription Indicator	ID Proof	This application is within VA and has FIPS 2.0 encryption.

4.1b List internal organizations information is shared/received/transmitted, the information shared/received/transmitted, and the purpose, and how the information is transmitted.

NOTE: Question 3.9b (second table) on Privacy Threshold Analysis should be used to answer this question.

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

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

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

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

Data Shared with Internal Organizations

IT system and/or Program office. Information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List PII/PHI data elements shared/received/transmitted.***	***Describe the method of transmittal***
Compensation and Pension Record Interchange (CAPRI)	To view Veteran exam appointments	Customer Names, SSN, Exam Appointment Information	Veterans Experience Integration Solution
Master Veteran Index MVI	Using the demographic data returned from the BGS service, MVI will return ICN and Data File Numbers (DFN) for the matching patient.	First Name, Last Name, SSN. MVI will return interface Change Notice ICN and Data File Numbers (DFN) for the matching patient.	Veterans Experience Integration Solution
Benefits Gateway Services BGS	This service retrieves veteran sensitivity levels and will be used when applying CRM security roles to the interaction history records. The data source is CORP DB.	Veteran sensitivity levels, Payment Details, Demographics, Addresses and Updates Contact History	Veterans Experience Integration Solution
Corporate Data Warehouse Corporate DB CORP DB	To view Veteran address, and relationships (spouse and next of kin)	Veteran address, and relationships (spouse and next of kin)	Veterans Experience Integration Solution
Beneficiary Identification and	To view Veteran insurance information	Veteran insurance information, SSN	Veterans Experience

IT system and/or Program office. Information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT system*	*List PII/PHI data elements shared/received/transmitted.*	*Describe the method of transmittal*
Records Locater Subsystem (BIRLS)			Integration Solution
Modern Award Processing Development (MAP-D)	To view Veteran contact history notes	Veteran contact history notes, SSN	Veterans Experience Integration Solution
SHARE	To view Veteran ratings, awards, and payments	Veteran ratings, awards, and payments, SSN	Veterans Experience Integration Solution
Finance and Accounting Services (FAS)	To view Veteran benefits payments	Veteran benefits payments	Veterans Experience Integration Solution
VA/DoD Identify Repository (VADIR)	To view veteran's US Citizenship Status, Country of Origin, Service Code and Address	Veteran's US Citizenship Status, Country of Origin, Service Code and Address	VA Reflection File Transfer Protocol (FTP)
Education	To view veteran education benefits flag and education transferred entitlement flag	Veteran Education Benefit Flag and Education Transferred Entitlement Flag	VA Reflection File Transfer (FTP)
Loan Guaranty (LGY)	To view veteran LGY flag information	Veteran LGY Flag	VA Reflection File Transfer Protocol (FTP)
Veterans Group Life Insurance (VGLI)	To view veteran VGLI effective date	Veteran VGLI Effective Date	VA Reflection File Transfer Protocol (FTP)
VA Profile	To view contact information	Address, Telephone, Email Address, Active Prescription Indicator, Disability Ratings	Veterans Experience Integration Solution

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

Discuss the privacy risks associated with the sharing of information within the VA network and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions in this section.).

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

Follow the format below:

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

Mitigation: CRM VOICE will adhere to information security requirements instituted by the VA OIT. Contractor and VA employees are required to take Privacy, HIPAA, and information security training annually.

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 List the external organizations (outside VA) that information shared/received. and information shared/received, and the purpose, and how the information transmitted and what measures are taken to ensure it is secure.

The sharing of information outside the agency must be compatible with the original collection. The sharing must be covered by an appropriate routine use in a SORN. If not covered, 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 IT System or External Program Office information is shared/received with	***List the purpose of information being shared / received / transmitted***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted)***	***List agreements such as: Contracts, MOU/ISA, BAA, SORN. 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				

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.

If no External Sharing listed on the table above, ***(State there is no external sharing in both the risk and mitigation fields).***

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: No external sharing

Mitigation: No external sharing

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 The notice provided to the individual before collection of the information. Please provide a copy and/or screen shot of a web notice of the notice as an Appendix-A 6.1 on the last page of the document. (A notice may include a posted privacy policy, a Privacy Act notice on forms,

notice given to individuals by the sources system, or a system of records notice published in the Federal Register.) If notice was not provided, explain why.

These questions are 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.

6.1a Provide the Privacy Notice provided to the public by this system or any source systems. Include a copy of the notice in Appendix A of the PIA, the Federal Register citation, or Privacy Statement from collection of information such as forms or surveys.

Information is collected directly from the Veteran, or their beneficiaries and the call center does not provide a written notice to callers. However, callers are notified in the call regarding their individual rights per VHA Directive 1605.1: Privacy and Release Information.

6.1b If notice was not provided, explain why.

Information is collected directly from the Veteran, or their beneficiaries and the call center does not provide a notice to callers. However, callers are notified in the call regarding their individual rights per VHA Directive 1605.1: Privacy and Release Information.

6.1c Provide how the notice provided at the time of collection meets the purpose of use for this system.

Information is collected directly from the Veteran, or their beneficiaries and the call center does not provide a notice to callers. However, callers are notified in the call regarding their individual rights per VHA Directive 1605.1: Privacy and Release Information.

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.

VHA Directive 1605.1 'Privacy and Release Information', Section 5 lists the rights of Beneficiaries to request the VHA to restrict the use and/or disclosures of individually identifiable health information to carry out treatment, payment, or health care operations. The caller must provide specific information before action can be taken, such as SSN. Beneficiaries have the right to refuse to disclose their SSNs to the VHA. The individual shall not be denied any right, benefit, or privilege provided by law because of refusal to disclose to VHA a SSN (please refer to the 38 Code of Federal Regulations CFR 1.575(a)).

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.

VHA Directive 1605.1: Privacy and Release Information, Section 5 lists the rights of Beneficiaries to request that the VHA restrict the uses and/or disclosures of individually identifiable health information to carry out treatment, payment, or health care operations.

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. (Work with your Privacy Officer (PO) to complete all Privacy Risk questions inside the document this section).

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

Principle of Transparency: This is referring to sufficient notice provided to the individual.

Principle of Use Limitation: The information used only for the purpose for which notice was provided either directly to the individual or through a public notice. The procedures in place must 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: CRM VOICE users do not adhere to information security requirements instituted by the VA OIT, if PII is disclosed, the trust and reputation in VA and the call centers could be harmed as a consequence.

Mitigation: Contractor and VA employees are required to take Privacy, HIPAA, and information security training annually.

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 The procedures that allow individuals to gain access to their information.

These questions are related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.

7.1a 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 VA Public Access Link-Home (efoia-host.com) to obtain information about FOIA points of contact and information about agency FOIA processes.***

Information typed and stored directly in the CRM tool is vetted by the NCC agents who ask Veterans to verify the information that they see (and collect) and along with information that is pulled and displayed from various legacy VA backend systems.

7.1b 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)?

System is not exempt.

7.1c 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?

VHA Directive 1605.1: Privacy and Release Information, Section 7(b) states the rights of Beneficiaries to request access to review their records. VA Form 10-5345a, Individual's Request for a Copy of Their Own Health Information, may be used as the written request requirement. 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 VHA 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.

The information collected from individuals who call the NCCs, if a correction is requested, then such a request must be in writing and it must adequately describe the specific information that 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 health care facility that maintains the record. VHA Directive 1605.1: Privacy and Release Information, Section 5 lists the rights of Beneficiaries to request that the VHA restrict the uses and/or disclosures of individually identifiable health information to carry out treatment, payment, or health care operations.

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.

Agents would notify the callers that they may change their information if the information presented is incorrect. VHA Directive 1605.1, Privacy and Release Information, Section 8 describes the Right to Request Amendment of Records : *"(1) An amendment request must be in writing, signed and must adequately describe the specific information the individual believes to be inaccurate (i.e., faulty or not conforming exactly to truth), incomplete (i.e., unfinished or lacking information needed), irrelevant (i.e., inappropriate or not pertaining to the purpose for which records were collected) or untimely (i.e., before the proper time or prematurely) and the*

reason for this belief. (a) A scanned, digital image or fax of a written, signed request will be accepted. (b) An amendment request submitted by Secure Messaging through a Patient Portal, such as MyHealtheVet, to the facility Privacy Officer explicitly that contains the required information and where the identity of the individual submitting the request can be authenticated will be accepted". This includes designated record sets, as provided in 38 CFR 1.579 and 45 CFR 164.526. 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 health care facility 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 VHA system of records, and the facility Privacy Officer, or designee, to be date stamped; and be 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. System of Records Notices provide a system Point of Contact. This PIA provides system owner to facilitate records correction.

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

This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Agents would notify the callers that they may change their information if the information presented is incorrect. VHA Directive 1605.1: Privacy and Release Information, Section 8 Right to Request Amendment of Records. This includes designated record sets, as provided in 38 CFR 1.579 and 45 CFR 164.526. 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 health care facility 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 VHA system of records, and the facility Privacy Officer, or designee, to be date stamped; and be 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. System of Records Notices provide a system Point of Contact. This PIA provides system owner to facilitate records correction.

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.*** *(Work with your Privacy Officer (PO) to complete all Privacy Risk questions in this section).*

Consider the following FIPPs below to assist in providing a response:
Principle of Individual Participation: The individual must be provided with the ability to find out whether a project maintains a record relating to them.

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

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

Follow the format below:

Privacy Risk: There is a risk that individuals whose records contain incorrect information may not obtain access to VOICE.

Mitigation: VOICE project staff would work with the affected individual and assist with opening an OIT Snow ticket for the individual.

Section 8. Technical Access and Security

The following questions are intended to describe technical safeguards and security measures. (Work with your ISSO to complete this section).

8.1 The procedures in place to determine which users may access the system, must be documented.

These questions are related to privacy control AR-7, Privacy-Enhanced System Design and Development.

8.1a Describe the process by which an individual receives access to the system?

The supervisor/Contracting Officer's Representative (COR) documents and monitors individual information system security training activities, including basic security awareness training and specific information system security training. This documentation and monitoring are performed through the use of the Talent Management System (TMS). Access to the system is granted to VA employees and contractors the supporting IT for the application after the supervisor/COR authorizes this access once requirements have been met. Only the IT system administrators authorized by VA IT will have the security role to modify the UDO application. This PIA will not result in technology protocol changes, additional controls, or single sign on, as per privacy control AR-7, Privacy-Enhanced System Design and Development. All UDO users must take the following steps before they are granted access to the system:
Individuals 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.

Individuals must have a completed security investigation.
After the training and the security investigation are complete, a request is submitted for access.

8.1b 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?

There are no other users from other government agencies that will need the access.

8.1c 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.

The number of user roles is subject to change while the system is developed. The following account types/roles are based on the job functions they perform.

Users- Have access to all data and workflows; view and edit.

Quality/Supervisors- Will have access to all data and workflows in addition to being able to look into a record or interaction without creating a new interaction.

System Analysts- Will have all access of lower levels in addition to being able to modify certain inputs of the system (Scripts, etc.)

System Admin-administrative functions such as maintenance, troubleshooting, upgrades, security, and monitoring.

8.2a. Will VA contractors have access to the system and the PII?

Yes, there will be restrictive access to contractors in production according to VA OIT instituted security requirements, VA Directives, and VA Privacy and Information Security.

8.2b. What involvement will contractors have with the design and maintenance of the system?

CRM VOICE team includes developers, UI/UX, and testers.

8.2c. Does the contractor have a signed confidentiality agreement? No

8.2d. Does the contractor have an implemented Business Associate Agreement for applicable PHI?
Yes, a BAA is active for PHI in accordance with the Health Insurance Portability and Accountability Act (HIPAA), the Health Information Technology for Economic and Clinical Health Act (HITECH), and the HIPAA Privacy, Security, Breach Notification, and Enforcement Rules ("HIPAA Rules"), 45 C.F.R. Parts 160 and 164, for the Use and Disclosure of Protected Health Information (PHI).

8.2e. Does the contractor have a signed non-Disclosure Agreement in place?
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.

Yes, VOICE has an NDA that all Contractors sign during Onboarding.

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 Information Security Rules of Behavior (RoB) prior to gaining access to any VA information system or sensitive information. The rules are included as part of the security awareness training that all personnel must complete via the VA's 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 obtained through electronic acknowledgment is tracked through the TMS system. All VA employees must complete annual Privacy 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 CIOs Executives, Senior Managers, CIOs and 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

8.4 The Authorization and Accreditation (A&A) completed for the system.

8.4a If Yes, provide:

1. *The Security Plan Status:* <<ADD ANSWER HERE>>
2. *The System Security Plan Status Date:* <<ADD ANSWER HERE>>
3. *The Authorization Status:* <<ADD ANSWER HERE>>
4. *The Authorization Date:* <<ADD ANSWER HERE>>
5. *The Authorization Termination Date:* <<ADD ANSWER HERE>>
6. *The Risk Review Completion Date:* <<ADD ANSWER HERE>>
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* <<ADD ANSWER HERE>>

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

8.4b If No or In Process, provide your ***Initial Operating Capability (IOC) date.***

System is in development. Pilot TBD for 2025. System Classification: Moderate

Section 9 – Technology Usage

The following questions are used to identify the technologies being used by the IT system or project.

9.1 Does the system use cloud technology? If so, what cloud model is being utilized?

If so, Does the system have a FedRAMP provisional or agency authorization? If the system does use cloud technology, but does not have FedRAMP authorization, explain how the Cloud Service Provider (CSP) solution was assessed and what FedRAMP documents and processes were used for the assessment in order to comply with VA Handbook 6517. Types of cloud models include: Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Commercial off the Shelf (COTS), Desktop as a Service (DaaS), Mobile Backend as a Service (MBaaS), Information Technology Management as a Service (ITMaaS). This question is related to privacy control UL-1, Information Sharing with Third Parties. ***(Refer to question 1.8 of the PTA)***

Yes, per PTA, CRM VOICE, a SaaS in Government Cloud - MAG with FedRAMP.

9.2 Does the contract with the Hosting 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). ***(Refer to question 3.3.1 of the PTA)*** *This question is related to privacy control AR-3, Privacy Requirements for Contractors, and Service Providers.*

Yes, information from PTA: The Azure Government General Support Global Operations Services are covered under the Microsoft – Azure for Government JAB FedRAMP ATO package ID F1209051525 and the VA associated ATO. The Microsoft Azure Government (includes Dynamics 365) SaaS Platform services are covered under the FedRAMP ATO for Microsoft Azure. Government (includes Dynamics 365) JAB FedRAMP ATO package ID F1603087869 and the associated VA CSP-ATO. The VA General Support Systems are covered under the VA Regions 1-6 General Support System (GSS) ATO.

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.

For CRM VOICE, no ancillary data is collected.

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 Azure Government General Support Global Operations Services are covered under the Microsoft – Azure for Government JAB FedRAMP ATO package. As the CSP, Microsoft maintains and monitors the MS Azure Government Cloud.

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).

No RPA is used.

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**
UL-1	Internal Use
UL-2	Information Sharing with Third Parties

Signature of Responsible Officials

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

MARVIS HARVEY

Digitally signed by MARVIS HARVEY
Date: 2025.01.28 13:21:08 -06'00'

Privacy Officer, Marvis Harvey

ALBERTINO ESTACIO

Digitally signed by ALBERTINO ESTACIO
Date: 2025.02.13 14:37:12 -08'00'

Information Systems Security Officer, Albert Estacio

IZEL CRUZ MAISONAVE

Digitally signed by IZEL CRUZ MAISONAVE
Date: 2025.01.28 15:59:30 -05'00'

Information Systems Owner, Izel Cruz Maisonave

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; screen shot of a website collection privacy notice).

HELPFUL LINKS:

Records Control Schedule 10-1 (va.gov)

General Records Schedule
https://www.archives.gov/records-mgmt/grs.html

National Archives (Federal Records Management):
https://www.archives.gov/records-mgmt/grs

VA Publications:
https://www.va.gov/vapubs/

VA Privacy Service Privacy Hub:
https://dvagov.sharepoint.com/sites/OITPrivacyHub

Notice of Privacy Practice (NOPP):
VHA Directive 1605.04
IB 10-163p (va.gov)