Privacy Impact Assessment for the VA IT System called:

Nintex Automation Cloud for Government -e

Office of Information Technology,

Product Delivery Service,

Digital Transformation Center

eMASS ID # 2083

Date PIA submitted for review:

4/4/2025

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Tonya Facemire	Tonya.Facemire@va.gov OITPrivacy@va.gov	202-632-8423
Information System Security Officer (ISSO)	Danny O'Dell	Danny.Odell@va.gov	650-495-5977
Information System Owner	Scottie Ross	Scottie.Ross@va.gov	478-595-1349

Abstract

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

Nintex Automation Cloud for Government (NACG) provides users an easy way to manage complex business processes through the use of workflows and forms without having to code. NACG's drag-and-drop designer provides the VA with a true citizen developer workflow and forms automation solution, enabling users to automate, scale, and improve business processes. With the ability to connect to other Software-as-a-Service (SaaS) products approved for use by the VA, such as Microsoft SharePoint Online, Box, and DocuSign, NACG users can incorporate products they use every day into their workflows and form development.

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?

Nintex Automation Cloud for Government (NAC-G) allows Veterans Affairs organizations to automate both simple and sophisticated business processes, such as approving and signing documents, or hiring and onboarding employees.

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 Controlled / non-VA Owned and Operated IS (Information System)

2. Information Collection and Sharing

C. 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?

Although workflows and forms will have individual's information pass through the product from almost all possible demographics within Veteran Affairs, no information is stored in the system.

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

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

Information collected is determined by the workflow designer based in their particular use case.

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

Information collected through Nintex Automation Cloud for Government workflows can be shared with various products such as Microsoft Office 365, DocuSign, Box, Microsoft Entra ID, Microsoft Azure Services, Salesforce, and Adobe Acrobat Sign for Government.

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

There are no modules/subsystems.

G. 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?

Nintex Automation Cloud for Government is a Software-as-a-Service.

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

H. What is the citation of the legal authority?

- Privacy Act of 1974, 5 U.S.C. § 552a (as amended)

- 38 United States Code (U.S.C.) §§ 5721-5728
- E-Government Act of 2002 (Pub. L.107-347), Data Security and Privacy
- Federal Information Security Management Act (FISMA)
- OMB M-06-15, Safeguarding Personally Identifiable Information (May 22, 2006)
- OMB M-03-22, "OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002

I. What is the SORN?

There are no SORNS applicable to Nintex Automation Cloud for Government. It is not a Privacy Act System of Records, as information about individuals is not retrieved from the system by a name or other personal identifier.

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

There are no SORNS applicable to Nintex Automation Cloud for Government. It is not a Privacy Act System of Records, as information about individuals is not retrieved from the system by a name or other personal identifier.

4. System Changes

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

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

I. 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
- ☒ 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)

Other PII/PHI data elements: Place of Birth, Emotional Support Animal, Biometric Identifiers

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?

Forms are sent directly to individuals such as Veterans or Dependents, VA Employees, Clinical Trainees, VA Contractors, or Volunteers to enter this information.

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

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.

The system does not currently collect or process PII from sources other than the individuals themselves.

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

No, this system does not create 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 system collects, stores, and transmits information in web forms* using the following technologies:

Collection:
Web forms with input validation for direct user data entry. Transmitted via secure socket layer over TLS.

Storage:
Encrypted relational database (e.g., Azure SQL) for PII storage using Transparent Data Encryption (TDE) on the databases and Storage account encrypted with Azure Storage Service Encryption (SSE).

Transmission:
HTTPS for all user interactions with the system's web interface and transmitted to any other systems identified above over HTTPS.

**Requests that use the browser for display.*

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?

Information is not collected on an OMB form.

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 system does not ingest information from other systems. This is the user's responsibility when populating the system with their information and it is their responsibility to update the system to be accurate.

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?

The system does not check for accuracy by accessing a commercial aggregator of information.

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

- Privacy Act of 1974, 5 U.S.C. § 552a (as amended)
- 38 United States Code (U.S.C.) §§ 5721-5728
- E-Government Act of 2002 (Pub. L.107-347), Data Security and Privacy
- Federal Information Security Management Act (FISMA)
- OMB M-06-15, Safeguarding Personally Identifiable Information (May 22, 2006)
- OMB M-03-22, "OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002

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

Consider the specific data elements collected and discuss the potential privacy risks and what steps, if any are currently being taken to mitigate those identified risks.

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

<u>Principle of Purpose Specification:</u> 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: The system collects, processes, and transmits PII and PHI on Veterans and on VA staff. If this information was breached or accidentally disclosed to inappropriate parties or the public, it could result in personal and financial harm to the individuals impacted and adverse negative effect to the VA.

Mitigation:
Minimization: The NAC-G system collects only the minimum necessary PII required to fulfill the VA's mission, aligning with the principles of Privacy by Design.

Encryption: PII is encrypted both at rest (using AES-256 encryption in Azure SQL Database and Azure Blob Storage) and in transit (using HTTPS with TLS 1.2 or higher).

Access Controls: Strict role-based access controls (RBAC) are implemented, ensuring that only authorized personnel can access specific data based on their roles and responsibilities within the system.

Purpose Limitation: Technical controls, including database views and stored procedures, are implemented to restrict data access and usage to only what is necessary for the intended purposes.

Audit Logs: The Nintex Automation Cloud system maintains detailed audit logs of all system activity, including data access, modifications, and potential security events. These logs are regularly reviewed to detect and investigate any unauthorized or suspicious activity.

Regular Security Assessments: Nintex Automation Cloud undergoes regular security assessments, including vulnerability scans and penetration testing, to identify and address potential security weaknesses that could expose 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 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.

**There is no external use of this business tool*

PII/PHI Data Element	Internal Use	External Use*
First and Last Name	End-user authentication	Not used
Social Security Number	Could be collected on a Nintex Form or through internal VA application sharing as part of a workflow that passes through this system	Not used
Personal Phone Numbers	Could be collected on a Nintex Form or through internal VA application sharing as part of a workflow that passes through this system	Not used
Personal Email Addresses	Could be collected on a Nintex Form or through internal VA application sharing as part of a workflow that passes through this system	Not used
Date of Birth	Could be collected on a Nintex Form or through internal VA application sharing as part of a workflow that passes through this system	Not used
Place of Birth	Could be collected on a Nintex Form or through internal VA application sharing as part of a workflow that passes through this system	Not used
Mother's Maiden Name	Could be collected on a Nintex Form or through internal VA application sharing as part of a workflow that passes through this system	Not used
Sex	Could be collected on a Nintex Form or through internal VA application sharing as part of a workflow that passes through this system	Not used
Mailing/Physical Address	Could be collected on a Nintex Form or through internal VA application sharing as part of a	Not used

	workflow that passes through this system	
Emergency Contact Info	Could be collected on a Nintex Form or through internal VA application sharing as part of a workflow that passes through this system	Not used
Next of Kin	Could be collected on a Nintex Form or through internal VA application sharing as part of a workflow that passes through this system	Not used
Race/Ethnicity	Could be collected on a Nintex Form or through internal VA application sharing as part of a workflow that passes through this system	Not used
Integrated Control Number	Could be collected on a Nintex Form or through internal VA application sharing as part of a workflow that passes through this system	Not used
Driver's License Number	Could be collected on a Nintex Form or through internal VA application sharing as part of a workflow that passes through this system	Not used
Vehicle License Plate Number	Could be collected on a Nintex Form or through internal VA application sharing as part of a workflow that passes through this system	Not used
Military History/Service Connection	Could be collected on a Nintex Form or through internal VA application sharing as part of a workflow that passes through this system	Not used
Financial Information	Could be collected on a Nintex Form or through internal VA application sharing as part of a workflow that passes through this system	Not used
Medical Record Number	Could be collected on a Nintex Form or through internal VA application sharing as part of a workflow that passes through this system	Not used

Medications	Could be collected on a Nintex Form or through internal VA application sharing as part of a workflow that passes through this system	Not used
Emotional Support Animals	Could be collected on a Nintex Form or through internal VA application sharing as part of a workflow that passes through this system	Not used
Biometric Identifiers	Could be collected on a Nintex Form or through internal VA application sharing as part of a workflow that passes through this system	Not used
Business Email Address	End-user authentication	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?

Data analysis is not conducted in this system.

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.

The system does not create or make available previously utilized information.

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?

All data in transit and at rest is encrypted with FIPS 140-2 validated cryptographic modules leveraging TLS 1.2 or higher.

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).

Any social security numbers are protected using encryption.

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

The system complies with FedRAMP Moderate control requirements and safeguard customer data in accordance with those requirements.

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?

Access to limited VA Business Data is determined by role. Only name and business email are stored in the system and accessible by those with Global Administrator access. No other PII data persists in the system.

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?

The active management of VA network and email accounts by End User Operations annually on regular end users in accordance with VA Handbook 6500 enables the VA to remove personnel who no longer require access. The VA also requires employees (Government and Contractors) to read and accept the VA Rules of Behavior (ROB) before access is granted to the VA network or email accounts.

2.4c Does access require manager approval?

No, access to the system does not require manager approval.

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

Other than the VA Business Data mentioned in section 2.4a, no other PII data elements are stored or tracked in the system.

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

The information is handled in accordance with the uses described above include mandatory online information security and Privacy and HIPAA training; face-to-face training for all incoming new employees conducted by the Information System Security Officer and Privacy Officer. All VA employees are required to complete annual Rule of Behavior training.

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

Other than name and business email address, no other PII data elements are retained in the system.

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 https://www.archives.gov/records-mgmt/grs? This question is related to privacy control DM-2, Data Retention and Disposal.

Information is not retained in the system once workflow is complete.

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?

No records are stored within the system.

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

No records are stored within the system.

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.

No records are stored within the system.

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.

PII is not used for research, testing or training.

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 in 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 contained in Nintex Automation Cloud will be retained for longer than is necessary to fulfill the VA mission. Records held longer than required are at greater risk of unauthorized access or being breached.

Mitigation: The entire process is encrypted in order to protect all data. Once workflow completes, all information from that workflow is purged from system. Additionally, access to view workflow progress is limited to administrators and the workflow owner, all of whom complete annual privacy training to ensure proper safeguarding of sensitive information.

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 Nintex Automation Cloud for Government-e consists of no 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 Nintex Automation Cloud for Government-e 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
N/A	N/A	N/A	N/A	N/A	N/A

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***
All administrations across the VA (VHA, VBA, NCA, OIT, VACO, etc.)	Dependent on end-user's form or workflow use case. VA employee designing the form is responsible for providing the purpose of information being collected and authorized use, sharing, dissemination of the information within the Privacy notice displayed on the form.	First and Last Name Social Security Number Personal Phone Numbers Personal Email Addresses Business Email Address Date of Birth Mailing/Physical Address Place of Birth Mother's Maiden Name Emergency Contact Info Next of Kin Sex Race/Ethnicity Integrated Control Number Driver's License Number Vehicle License Plate Number Military History/Service Connection Financial Information Medical Record Number	All data in transit and at rest is encrypted with FIPS 140-2 validated cryptographic modules leveraging TLS 1.2 or higher.

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*
		Medications Emotional Support Animals Biometric Identifiers	
Microsoft Entra ID-E (eMASS ID# 2628)	VA Active Directory Services System. VA employee designing the form is responsible for providing the purpose of information being collected and authorized use, sharing, dissemination of the information within the Privacy notice displayed on the form.	First and Last Name Personal Phone Numbers Personal Email Addresses Business Email Address Mailing/Physical Address Sex	All data in transit and at rest is encrypted with FIPS 140-2 validated cryptographic modules leveraging TLS 1.2 or higher.
Box Enterprise Cloud Content Collaboration Platform-E (eMASS ID# 1170)	Used as part of business process. VA employee designing the form is responsible for providing the purpose of information being collected and authorized use, sharing, dissemination of the information within the Privacy notice displayed on the form.	First and Last Name Social Security Number Personal Phone Numbers Personal Email Addresses Business Email Address Date of Birth Mailing/Physical Address Place of Birth Mother's Maiden Name Emergency Contact Info Next of Kin Sex Race/Ethnicity Integrated Control Number Driver's License Number Vehicle License Plate Number Military History/Service Connection Financial Information Medical Record Number Medications Emotional Support Animals Biometric Identifiers	All data in transit and at rest is encrypted with FIPS 140-2 validated cryptographic modules leveraging TLS 1.2 or higher.
Microsoft Azure Services (eMASS ID# 2338)	Dependent on end-user's form or workflow use case. VA employee designing the form is responsible for	Personal Email Addresses Business Email Address Date of Birth Mailing/Physical Address Place of Birth	All data in transit and at rest is encrypted with FIPS 140-2 validated

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*
	providing the purpose of information being collected and authorized use, sharing, dissemination of the information within the Privacy notice displayed on the form.	Mother's Maiden Name Emergency Contact Info Next of Kin Sex Race/Ethnicity Integrated Control Number Driver's License Number Vehicle License Plate Number Military History/Service Connection Financial Information Medical Record Number Medications Emotional Support Animals Biometric Identifiers	cryptographic modules leveraging TLS 1.2 or higher.
Microsoft Office 365 Multi-Tenant (MO365MT) (eMASS ID# 0079)	Dependent on end-user's form or workflow use case. VA employee designing the form is responsible for providing the purpose of information being collected and authorized use, sharing, dissemination of the information within the Privacy notice displayed on the form.	First and Last Name Social Security Number Personal Phone Numbers Personal Email Addresses Business Email Address Date of Birth Mailing/Physical Address Place of Birth Mother's Maiden Name Emergency Contact Info Next of Kin Sex Race/Ethnicity Integrated Control Number Driver's License Number Vehicle License Plate Number Military History/Service Connection Financial Information Medical Record Number Medications Emotional Support Animals Biometric Identifiers	All data in transit and at rest is encrypted with FIPS 140-2 validated cryptographic modules leveraging TLS 1.2 or higher.
Salesforce Government Cloud Plus - Enterprise (eMASS ID# 1295)	Dependent on end-user's form or workflow use case. VA employee designing the form is responsible for providing the purpose	First and Last Name Social Security Number Personal Phone Numbers Personal Email Addresses Business Email Address Date of Birth	All data in transit and at rest is encrypted with FIPS 140-2 validated cryptographic

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*
	of information being collected and authorized use, sharing, dissemination of the information within the Privacy notice displayed on the form.	Mailing/Physical Address Place of Birth Mother's Maiden Name Emergency Contact Info Next of Kin Sex Race/Ethnicity Integrated Control Number Driver's License Number Vehicle License Plate Number Military History/Service Connection Financial Information Medical Record Number Medications Emotional Support Animals Biometric Identifiers	modules leveraging TLS 1.2 or higher.
Docusign Federal-Enterprise (eMASS ID# 1169)	Dependent on end-user's form or workflow use case. VA employee designing the form is responsible for providing the purpose of information being collected and authorized use, sharing, dissemination of the information within the Privacy notice displayed on the form.	First and Last Name Social Security Number Personal Phone Numbers Personal Email Addresses Business Email Address Date of Birth Mailing/Physical Address Place of Birth Mother's Maiden Name Emergency Contact Info Next of Kin Sex Race/Ethnicity Integrated Control Number Driver's License Number Vehicle License Plate Number Military History/Service Connection Financial Information Medical Record Number Medications Emotional Support Animals Biometric Identifiers	All data in transit and at rest is encrypted with FIPS 140-2 validated cryptographic modules leveraging TLS 1.2 or higher.
Adobe Acrobat Sign for Government-E (eMASS ID# 2564)	Dependent on end-user's form or workflow use case. VA employee designing the	First and Last Name Social Security Number Personal Phone Numbers Personal Email Addresses	All data in transit and at rest is encrypted with FIPS 140-2

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*
	form is responsible for providing the purpose of information being collected and authorized use, sharing, dissemination of the information within the Privacy notice displayed on the form.	Business Email Address Date of Birth Mailing/Physical Address Place of Birth Mother's Maiden Name Emergency Contact Info Next of Kin Sex Race/Ethnicity Integrated Control Number Driver's License Number Vehicle License Plate Number Military History/Service Connection Financial Information Medical Record Number Medications Emotional Support Animals Biometric Identifiers	validated cryptographic modules leveraging TLS 1.2 or higher.

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: There is a risk that sensitive Personally Identifiable Information (PII) could be improperly accessed or unintentionally disclosed to unauthorized individuals.

Mitigation: All VA personnel complete annual training Privacy and Security Training to ensure proper handling of PII.

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	N/A	N/A	N/A	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: There is no external sharing.

Mitigation: There is 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.

Privacy Notice not provided.

6.1b If notice was not provided, explain why.

There are many different use cases, all of which need input by the business team with designer permissions within NAC-G that create the forms for their specific use case. The VA employee designing the form is responsible for providing the purpose of information being collected and authorized use, sharing, and dissemination of the information within the Privacy notice displayed on the form.

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

Each form should be designed with a privacy act notice that includes the explicit purpose of data collection by the NAC-G system.

6.2 Do individuals have the opportunity and right to decline to provide information? If so, is a penalty or denial of service attached?

This question is directed at whether the person from or about whom information is collected can decline to provide the information and if so, whether a penalty or denial of service is attached. This question is related to privacy control IP-1, Consent, IP-2, Individual Access, and IP-3, Redress.

If form users elect to not utilize the form to provide their information to the respective VA business team, secondary manual processes could accomplish the same purpose. If the user does not agree to the conditions of the privacy act statement, then they cannot use the system.

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.

VA employee designing the form is responsible for providing the purpose of information being collected and authorized use, sharing, dissemination of the information within the Privacy notice displayed on the form. When accepting the privacy act statement, the user agrees to all of the authorized use cases listed on the privacy act statement.

6.4 <u>PRIVACY IMPACT ASSESSMENT: Notice</u>

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:

<u>Principle of Transparency:</u> This is referring to sufficient notice provided to the individual.

<u>Principle of Use Limitation:</u> 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: There is a risk when a Nintex Form is created that the form designer will not provide the proper privacy notice to the recipient(s) of the form.

Mitigation: All VA users are provided with VA Rule of Behavior training annually which gives guidance on the proper use of privacy sensitive information and how to protect it. When VA users request access to Nintex Automation Cloud, they are provided a link to the product governance that also provides an overview of their responsibility to provide the proper privacy notice on forms they've designed, as needed. There is no oversight that would identify errors.

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.***

Standard FOIA/Privacy Act practices maintained by the VA. Privacy data not stored or maintained within the system. It is offloaded and stored in external systems as mentioned in section 4 above.

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)?

The system is configured by VA users to manage forms and workflows. The data entered into the form, through which the VA is required to configure captures that form information and stores it within the external (to NAC-G) repository of choice. Customers will not access the NAC-G system directly to update or provide information.

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?

The system is not a privacy act system. Consumer must work with applicable business unit listed on the privacy notice configured for each form to amend or correct the information input into the form. NAC-G does not store this information and does not provide a user interface intended for this use case.

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 consumer must work with applicable business unit listed on the privacy notice configured for each form to amend or correct the information input into the form. NAC-G does not store this information and does not provide a user interface intended for this use case.

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.

The consumer must work with applicable business unit listed on the privacy notice configured for each form to amend or correct the information input into the form. NAC-G does not store this information and does not provide a user interface intended for this use case.

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.

The consumer must work with applicable business unit listed on the privacy notice configured for each form to amend or correct the information input into the form. NAC-G does not store this information and does not provide a user interface intended for this use case.

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:

- PII Sensitivity: The system collects sensitive PII, including those called out in section 4 above, this creates privacy risks related to unauthorized access, disclosure, or misuse.
- Identifiability: Collected PII elements could potentially be combined to re-identify individuals, exposing them to privacy risks.

Mitigation:

- Minimization: The system adheres to the principle of data minimization, collecting only the PII strictly necessary for its core functions.
- Encryption & Access Controls: PII is protected with strong encryption at rest and in transit. Role-based access controls (RBAC) enforce the principle of least privilege.
- Purpose Limitation: Technical and procedural safeguards are in place to prevent the use of PII for purposes beyond the explicitly stated mission of the system.
- Transparency: Clear privacy notices inform individuals about information collection, use, and their rights regarding their data.
- Auditing & Logging: Regular audits and detailed logging mechanisms help detect and investigate potential privacy breaches.

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?

Access to PII is granted by the VA based on their internal policies and procedures and a valid need to know. Typically for other VA projects it is accomplished via a Service Now (SNOW) ticket being put in requesting access and then the VA ISSO/ISSM for the system would put them in the proper AD group to access via SSO or federation. The VA Agency administrator would then provide the user with the proper roles inside of the application.

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?

No. Information is not shared outside of the VA.

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.

Participant: Can leverage the NAC-G system and submit forms but cannot create and modify workflows or assign connection permissions.

Designer: Can create and modify workflows and enable limited connections

Administrator: Can authorize connections with external sources, such as those listed in section 4.0 and enable forms functionality for the tenant.

None of these roles provide users with the ability to modify or change information as the NAC-G is just the mechanism for delivering data to other systems via forms functionality.

8.2. Contractor signed Non-Disclosure Agreement (NDA), Business Associate Agreement (BAA) etc. in place.

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.

8.2a Has a contractor confidentiality agreement, Business Associate Agreement (BAA), or a Non-Disclosure Agreement (NDA) been developed for contractors who work on the system?

No contractor confidentiality agreement, BAA or NDA has been developed for this system as no contractors work on it.

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

VA contractors will have access to the system but not to PII data.

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

No contractor involvement with design and maintenance for this system.

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.

In addition to annual VA privacy and security training, the system's governance SharePoint site offers additional guidance to users regarding PII.

All CSP users take the following training: Security and privacy awareness training, insider threat training, information spillage training, counterfeit prevention awareness training and role-based training on an annual basis.

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

8.4a If completed, provide:

1. *The Security Plan Status:* Approved
2. *The System Security Plan Status Date:* 12/1/2023
3. *The Authorization Status:* Authorization to Operate (ATO)
4. *The Authorization Date:* 3/11/2024
5. *The Authorization Termination Date:* 6/14/2025
6. *The Risk Review Completion Date:* 3/25/2025
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.

8.4b If not completed or In Process, provide your ***Initial Operating Capability (IOC) date.***

<<ADD ANSWER HERE>>

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)***

This system is a Software as a Service (SaaS) that uses cloud technology. This system is FedRAMP Authorized.

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.*

Nintex (Azure Government Cloud) has agreement in place with VA with Contract Number NNG15SD33B.

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, none of the data is mapped to the VA or any of the other customers.

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.

All VA sensitive information shall be protected at all times in accordance with local security field office System Security Plans (SSP's) and Authority to Operate (ATO)'s for all systems/LAN's accessed while performing the tasks detailed in this Product Description.

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).

System does not utilize RPA.

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

TONYA FACEMIRE

Digitally signed by TONYA FACEMIRE
Date: 2025.04.14 20:12:57 -04'00'

Privacy Officer, Tonya Facemire

DANNY O'DELL

Digitally signed by DANNY O'DELL
Date: 2025.04.14 15:06:12 -07'00'

Information System Security Officer, Danny O'Dell

SCOTTIE ROSS

Digitally signed by SCOTTIE ROSS
Date: 2025.04.15 08:31:07 -04'00'

Information System Owner, Scottie Ross

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)