Privacy Impact Assessment for the VA IT System called:

Saviynt Enterprise Identity Cloud (EIC)

Office of Information & Technology

Office of Information & Technology – PES ICAM

eMASS ID # 2630

Date PIA submitted for review:

04/29/2025

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Gina Siefert	Gina.Siefert@va.gov	224-558-1584
Information System Security Officer (ISSO)	Martin DeLeo	Martin.Deleo@va.gov	202-299-6495
Information System Owner	Chino Walters	Chino.Walters@va.gov	(202) 461-0452

Abstract

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

Saviynt provides identity lifecycle management, access request management, reviews, and certifications, advance Zero-Trust Architecture for VA. This product will improve VA security and remediate items from the 2022 FISMA Audit (Notice of Findings and Recommendations (NFR) 4) while modernizing VA's Identity, Credential and Access Management (ICAM) infrastructure.

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?

Saviynt Enterprise Identity Cloud (EIC) is a Software-as-a-Service (SaaS) cloud-based tool for Identity Governance Administration (IGA), hereafter referred to as Saviynt. This tool provides security administrators the ability to manage user identities and access across VA while reducing risk of unnecessary or excessive user access to applications, systems, and data. The IGA tool centralizes identity management, policy, and access controls, and it will collect the information necessary for provisioning and deprovisioning users, their roles, entitlements, and applications. This tool allows for each individual user to have the appropriate access at the appropriate time while maintaining separation of duties (SOD). The tool provides access reviews and certifications for auditing purposes. The tool will flag risky access provisioning, such as potential SOD violations, and assign risk scores for approvers to see when determining whether access should be provisioned to the user. This system will allow the VA to address audit findings and material weaknesses, improve the VA security, and safeguard Veteran information. Moreover, this tool will increase government cost savings by allowing consolidation and decommissioning of enterprise legacy systems that are costly to maintain and operate. Saviynt improves government efficiency and employee productivity by reducing the number of resources necessary to provision and deprovision users and their access, eliminating non-standard and manual processes that take days or weeks with automated and scalable workflows, decreasing the number of duplicate and orphaned accounts.

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.

Office of Information & Technology

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?

At this current stage of a phased rollout, the expected number of individuals impacted is 10,000 workforce employees. This tool is for internal workforce users only and will in later phases be rolled out at an enterprise level, encompassing up to an estimated 750,000 total individuals of the VA workforce.

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?

Saviynt is an Identity Governance Administration (IGA) SaaS product that provides the ability to manage workforce identities, their entitlements, and access to resources, thereby increasing the VA's security posture. This system collects information to reduce the risk of unnecessary or excessive user access to applications, entitlements, systems, and data. It centralizes identity management, policy, access controls, and access certifications while providing automated workflows to improve the timeliness and accuracy of Joiner-Mover-Leaver and auditing processes. The information collected involve identity data fields to manage access, entitlements, and perform audits:

- Name (First, Middle, Last)
- Business Display Name
- Business Email Address
- SEC ID (Business)
- Business Mailing Address
- Business Phone Number

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

Saviynt is a SaaS based solution that offers Identity Management and Identity Governance in the FedRAMP Moderate cloud environment. In its secure location, it holds Identity and access information to provision access to resources that users need to access within the VA. This includes but not limited to username, email, manager, roles and access rights. Saviynt integrates with enterprise sources of truth to gather this information and passing the relevant information to downstream targets so that users have the correct amount on access. Saviynt does not pass any other information beyond identity and access data to any other systems.

Information shared with Saviynt comes from Master Person Index (MPI) and Access Provisioning Deprovisioning System (APDS) as authoritative sources for the relevant identity data fields. MPI provides Name and Display Name fields, and APDS provides the Business Email Address, Mailing Address, Phone number, and SEC ID. This information is to allow the Saviynt system to conduct audits and manage application provisioning/deprovisioning and entitlements.

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

Saviynt will gather identity information from MPI and APDS to gather user base data. After that, the goal will be to integrate with as many applications as possible to automate provisioning of access based on defined business policies and roles. Saviynt processes users, accounts, roles and entitlements. Saviynt does not pass any other information beyond identity and access data to any other systems.

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?

This system is not operated in more than one site.

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

H. What is the citation of the legal authority?

The citation of legal authority is.5 U.S.C. 301; 38 U.S.C. 501; 40 U.S.C. 11331; 44 U.S.C 3544; Executive Order 9397; Homeland Security Presidential Directive 12; Federal Information Processing Standard 201–1.

I. What is the SORN?

The SORN that will cover VA Employees, Contractors, and Affiliates is: **146VA005Q3**/73 FR 16093 Department of Veterans Affairs Identity Management System (VAIDMS)-VA (3/26/2008) https://www.govinfo.gov/content/pkg/FR-2008-03-26/pdf/E8-6120.pdf

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

This system is not in the process of being modified.

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)
  - Business Display Name
  - SEC ID (Business)
  - Business Mailing Address
  - Business Phone Number

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 is collected from VA authoritative sources and applications to manage user identities, entitlements, access, and perform audits. This management includes the abilities for approving or denying access requests based on roles, providing safeguards and levels of approval for high risk requests, and an ability to revoke unnecessary access or entitlements.

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.

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

This information from VA authoritative sources is needed to ensure that the right individual has the right access at the right time. Business Name, Business Email Address, and Business Sec ID will allow employees to request access as well as managers to review and approve such requests. This system will allow VA to prevent or remove toxic combinations of risky access, ensure separation of duties for employees, and provide audit trails for access reviews at application level. Entitlements may be based on the employee's role, access need, and to support the business organizations they are associated with.

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

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?

Information is collected from authoritative sources to include MPI and APDS that is accessed through a secure API connection.

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 a 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.

All information will be collected from authoritative sources, namely MPI and APDS, and that information will be reflected in Saviynt. In addition, each connected application will have a reconciliation process that validates actual access to the expected access that Saviynt defines. VA will retain the responsibility for data integrity.

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?

Saviynt does not use a commercial aggregator to check for accuracy.

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

The full legal authority for operating the system is provided under:

- No. 104---231, 110 Stat. 3048
- 5 U.S.C. § 552a, Privacy Act of 1974, As Amended
- Public Law 100---503, Computer Matching and Privacy Act of 1988
- E---Government Act of 2002 § 208
- Federal Trade Commission Act § 5
- 44 U.S.C. Federal Records Act, Chapters 21, 29, 31, 33
- Title 35, Code of Federal Regulations, Chapter XII, Subchapter B
- OMB Circular A---130, Management of Federal Information Resources, 1996
- The legal authority is 38 U.S.C. 7601-7604 and U.S.C 7681-7683 and Executive Order 9397

The SORN that will cover VA Employees, Contractors, and Affiliates is:
146VA005Q3/73 FR 16093 Department of Veterans Affairs Identity Management System (VAIDMS)-VA (3/26/2008) https://www.govinfo.gov/content/pkg/FR-2008-03-26/pdf/E8-6120.pdf

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

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

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

Principle of Purpose Specification: 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: Data collected by Saviynt contains PII and other sensitive information. Due to the sensitive nature of this data, there is a risk that, if the data were accessed by an unauthorized individual or otherwise breaches, serious harm or even identity theft may result in a significant financial burden to address impact of stolen identity.

Mitigation: All access to Saviynt is controlled by user accounts and roles. Users are only allowed to see organizations and functions that they are approved to access. In addition, data is secured by encryption by TLS AES256 in transit and sensitive PII data is encrypted at Rest prior to storing in the DB.

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	For identification purposes	Not Used
Business Display Name	For email templates, alerts	Not Used
Business Email Address	For identification and notification purposes	Not Used
SEC ID (Business)	For identification purposes	Not Used
Business Mailing Address	For identification purposes	Not Used
Business Phone Number	For identification purposes and notification purposes	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?

The analytics engine is configurable to report and query on any data within the Saviynt system. It will generate access reports, outliers and risk scores as well as certification reporting.

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.

This system does not create new information on individuals.

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?

TLS for data in Transit and Encryption for data at Rest. In addition, all access to data is governed by access policy.

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).

This system is not collecting, processing or retaining SSNs.

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

This system does not process PHI. PII is safeguarded in accordance with OMB Memorandum M-06-15, Saviynt has implemented the following measures leveraging the protections described above:

Strong encryption: Encrypting data in-transit ensures that PII is protected from interception. This meets the requirement to encrypt data when transmitted over public networks, as outlined in the OMB memorandum.

FedRAMP Compliance: Saviynt's adherence to FedRAMP moderate standards means that it complies with rigorous security and privacy controls that are crucial for protecting sensitive information like PII. These controls include measures for incident response, continuous monitoring, and vulnerability management.

Secure API Communication: By ensuring all API communications are encrypted using TLS, Saviynt safeguards PHI and PII when interfacing with other services and applications, protecting data integrity and confidentiality.

Continuous Monitoring and Incident Response: Saviynt's continuous monitoring for security threats and its incident response plan allow for the quick identification and mitigation of any breaches involving PHI and PII. This proactive approach is essential for maintaining data security and compliance with federal guidelines.

Regular Audits and Compliance Checks: Regular audits and compliance checks, as part of Saviynt's FedRAMP compliance, ensure that security measures are consistently applied and effective in protecting PHI and PII. These audits help identify any potential vulnerabilities and ensure ongoing adherence to OMB M-06-15 requirements.

Endpoint Security: Securing endpoints involved in the transmission of PHI and PII, through encryption and secure configurations, prevents unauthorized access and data breaches at the device level.

By implementing these measures, Saviynt can effectively safeguard PHI and PII in accordance with OMB Memorandum M-06-15, ensuring the confidentiality, integrity, and security of sensitive information.

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.

AT-1: Policies and Procedures

AT-2: Literacy Training and Awareness

AT-3: Role-based Training

PL-4: Rules of Behavior

AC-2(13): Disable Accounts for High-risk Individuals

AT-1: Saviynt has documented its security awareness and training policies in the Saviynt Security Awareness & Training Policy, version 3.3 dated July 15, 2022. The policy addresses:

- Purpose and need for security policy;
- Scope of systems, people, and resources to which the policy applies;
- Roles and responsibilities for approval and maintenance with the policy
- Management commitment of Saviynt Leadership and coordination between corporate security, product security, labs, and other security partners, and compliance requirements to which Saviynt staff must adhere.

The Saviynt Security Awareness & Training Policy is reviewed and maintained by the Information Security Team. Updates to the policy are approved by the Director, InfoSec (Policy Manager) team and distributed to all employees via the Google Drive.

AT-2: Saviynt documents lessons learned and evaluates what works and what does not work from a threat detection and investigation standpoint. Saviynt then implements corrective action plans based on lessons learned in order to try to avoid such incidents in the future. Whenever a major change occurs within Saviynt, the HR team conducts refresher awareness training. The Information Security Team validates and determines courses.

AT-3: Saviynt provides role-based training through KnowBe4 before key roles (i.e., developers, security, system admins, etc.) access the FedRAMP environment. Saviynt provides annual refreshes of role-based training.

PL-4: Saviynt establishes and makes readily available to all personnel the Saviynt's Rules of Behavior which details the rules for those that have access to the FedRAMP boundary.

In addition, all Saviynt staff are required to sign confidentiality and non-disclosure agreements (NDA), at the time of hire as a condition for employment. Staff are required to resign their NDAs every three years, confirming that they understand and agree to these security-related expectations prior to gaining access to the Saviynt network.
The customer is responsible for ensuring that their users acknowledge and sign the organization's rules of behavior for their instance of Enterprise Identity Cloud.

AC-2(13): For AWS environment, GuardDuty and Security Hub monitor activity for possible malicious activity - monitored insights and GuardDuty alerts:

- AWS principals with suspicious access key activity
- AWS resources that are associated with malware
- AWS resources associated with cryptocurrency issues
- AWS resources with unauthorized access attempts
- IAM users with suspicious activity
- IAMUser/AnomalousBehavior(Exfiltration)

- IAMUser/AnomalousBehavior(Impact)
- IAMUser/AnomalousBehavior(RootCredentialUsage)
- IAMUser/InstanceCredentialExfiltration(UnauthorizedAccess)

CloudOps and Information security team receive alerts from Security Hub and GuardDuty to review and then implement user disablement after review and confirmation of activity.

EIC Rules: The "Enterprise Identity Cloud Administration Guide describes using Rules as a mechanism for automating account disable actions based on predefined conditions. Using AWS CloudTrail Alerts and CloudWatch Log Alerts, these rules can apply to high-risk individuals, and Saviynt could utilize this functionality to disable accounts based on a high-risk condition:

- User logs in User performs too many privileged activities
- User fails to login too many times with the wrong credentials
- User has AWS CloudTrail or CloudWatch Alerts from a blocked IP CIDR range

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?

Yes.

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.

Yes, this information is critical in order to complete audits regarding user access, prevention of toxic combinations of access, and create a paper trail for compliance requirements.

2.4a How is access to the PII determined?

Access to the system is governed by a need to know. All those with access have been trained in Privacy and Information Security and have signed Rules of Behavior and are required to comply with VA Directive 6001.

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?

Saviynt operates under the OIT Standard Operating Procedure (SOP), Infrastructure Operations, Network Operations Network Access Control procedures. It also adheres to National Institutes of Standards and Technology (NIST) Special Publication 800-53 Revision 5, and VA 6500 directives in order to protect confidentiality, integrity and availability of the information processed, stored and transmitted. As a FedRAMP Moderate SaaS system with approved Authority to Operate (ATO), there are numerous procedures & controls in place inclusive of

System Security Plan (SSP), Configuration Management Plan (CMP), Plan of Action and Milestones, Information System Contingency Plan (ISCP), Control Family Policy and Procedures, as well as other relative identification and authentication and access control documentation. The security-related areas include access control; awareness and training; audit and accountability; certification, accreditation, and security assessments; configuration management; contingency planning; identification and authentication; incident response; maintenance; media protection; physical and environmental protection; planning; personnel security; risk assessment; systems and services acquisition; system and communications protection; system and information integrity; and privacy.

2.4c Does access require manager approval?

VA Employees require manager approval for access to VA information systems per VA policy. VA employees are bound by VA Directive 6500 and other policies that define role-based access to VA systems. These requirements ensure that access is granted based on necessity, security , and adherence to policy, safeguarding government systems and data.

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

Yes, access is tracked through logging. Any administrative user's activities are tracked when accessing the system.

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

The Information System Owner (ISO), the System Steward, and the Authorizing Official (AO) is responsible for ensuring eMASS has identified safeguards with the applicable security and privacy control requirements met with the provided evidence.

Although Saviynt's SaaS platform meets FedRAMP Medium standards the government agency remains responsible for protecting the PII it manages within the platform. The Accountable Official identified in the Authority to Operate (ATO) bears final authority for PII monitoring. Overall, VA Directive 6502 is applicable to all employees and provides guidance for protecting PII and ensuring compliance with privacy laws, regulations, and policies. The directive applies to all VA employees, contractors, and anyone else who handles PII on behalf of the VA.

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

The information retained in the system includes SEC ID as well as the following fields covered under the Rolodex exception. This information will be used for business operations and management:

- Name (First, Middle, Last)
- Business Display Name
- Business Email Address
- Business Mailing Address
- Business Phone Number

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.

Records relating to persons covered by this system are retained in accordance with General Records Schedule 18, Item 17. Unless retained for specific, ongoing security investigations, and in accordance with NARA, all of the PIV collected data will be retained for a minimum of 7.5 years beyond the term of employment, unless otherwise directed.

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

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

Records relating to persons covered by this system are retained in accordance with General Records Schedule 18, Item 17. Unless retained for specific, ongoing security investigations, and in accordance with NARA, all of the PIV collected data will be retained for a minimum of 7.5 years beyond the term of employment, unless otherwise directed. The Retention record in the SORN is available at https://www.govinfo.gov/content/pkg/FR-2008-03-26/pdf/E8-6120.pdf.

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.

Saviynt uses the Saviynt ATO, and the information is based on the Saviynt environment. All data cached/stored by Saviynt is deleted based upon reaching the deletion timelines.

Saviynt provides capabilities to enable automatic or on-demand PII erasure based on user inactivity, customizable through analytics queries. It also allows for policy exceptions and regional adaptations, ensuring compliance with privacy laws. This elimination of SPI is in accordance with VA Handbook 6500, Data Minimization and Retention, which states VA will retain PII for only as long as necessary to fulfill the specified purpose(s).

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.

Saviynt does NOT use PII for testing information systems or pre-production prior to deploying to production nor does it utilize PII for training or research.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

Discuss the risks associated with the length of time data is retained and what steps, if any, are currently being taken to mitigate those identified risks. (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: The risk to maintaining data within Saviynt for a longer period than what is needed or required is that the longer information is kept, the greater the risk that information will be compromised, unintentionally released, or breached.

Mitigation: The system only retains information long enough to manage and process identity governance administration, including access requests, approvals, and audits. Saviynt is housed in a secure AWS Gov Cloud using the Saviynt ATO. The information is based on the Saviynt ATO FISMA Moderate environment. All data cached/stored by Saviynt is deleted upon reaching the deletion timeframes.

Records relating to persons covered by this system are retained in accordance with General Records Schedule 18, Item 17. Unless retained for specific, ongoing security investigations, and in accordance with NARA, all of the PIV collected data will be retained for a minimum of 7.5 years beyond the term of employment, unless otherwise directed.

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 Saviynt consists of 1 key component (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 Saviynt 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
All elements are related to Saviynt.User (pushed from VA Master Person Index (VA-MPI)) via Saviynt AP	Yes	Yes	• Name (First, Middle, Last) • Business Display Name • Business Email Address • SEC ID (Business) • Business Mailing Address • Business Phone Number	Verify and manage identity	Saviynt Servers are hosted on AWS Gov Cloud and inherit security controls up to the Application Layer. Saviynt uses a firewall and load balancers on their servers and Splunk for application monitoring. Saviynt connects to VA MPI through VAAFI. MPI uses the VA Authentication Federation Infrastructure (VAAFI) security infrastructure to enforce access and compliance policies. For more information on VAAFI and/or VA MPI VAAFI integration, see the "Standard Process for VA MPI Integration via VAAFI.DOCX" document and also at http://www.va.gov/EAUTH/. MPI also has security controls in place outlined in Section 4.2.

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***
VA Master Person Index (VA-MPI)	Purpose is to validate user identity and access	• Name (First, Middle, Last) • Business Display Name	IAM VA MPI utilization of Saviynt User API (Rest)
Account Provisioning and Deprovisioning System (APDS)	Purpose is to validate user identity and access	• Business Mailing Address • Business Email Address • SEC ID (Business) • Business Phone Number	IAM VA MPI utilization of Saviynt User API (Rest) Simple Object Access Protocol (SOAP) or Representational State Transfer (REST) over Hypertext Transfer Protocol Secure (HTTPS) using Secure Socket Layer (SSL) encryption and Certificate exchange

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: All parties who have access to the VA system may inappropriately access and misuse the data.

Mitigation: Existing mitigation techniques used to protect privacy from internal sharing and disclosure risks, such as training, system log monitoring and adherence to VA Directive 6500 will suffice as mitigation, since there is no increased risk. Risk increases with the number of people having access to protected information. However, this tool will ensure that audits are completed regularly to review access and provide needed checks to ensure only authorized users have access to information and resources needed for their roles. This tool will also reduce the risk of toxic combinations of access and flag potential separation of duties violations for review.

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.

Notice is provided within this PIA and the governing SORN. As this system is for internal workforce users, privacy statements would also be found on the web or paper forms completed as part of internal onboarding, such as the Privacy Act Statement included in the form OMB No. 3206-0182.

6.1b If notice was not provided, explain why.

Notice is provided.

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

This system is used for governance and management of internal workforce identities and to ensure that access is restricted to authorized individuals. The Privacy notice is provided in appendix A in accordance with the following System of Records Notices (SORN).

The SORN that will cover VA internal workforce users is:
146VA005Q3/73 FR 16093 Department of Veterans Affairs Identity Management System (VAIDMS)-VA (3/26/2008) https://www.govinfo.gov/content/pkg/FR-2008-03-26/pdf/E8-6120.pdf

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

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

Yes, the individual user has the right to decline. However, information is required to verify identity for access to authorized VA applications, systems, and resources. VA users must use VA systems so that access is limited to what is the minimum necessary for their roles. There

is no penalty for refusal to verify identity; however, if we are unable to verify identity without the information, the user will not be able to access any VA internal workforce applications, systems, and resources. Having identity information is a basic assumption and requirement of Saviynt.

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.

The individual has the right to consent as outlined within the System of Records Notice 146VA005Q3 for internal workforce users. All requests must be in writing and adequately describe the specific information the individual believes to be inaccurate, incomplete, irrelevant, or untimely and the reason for this belief. The written request needs to be mailed or delivered to the VA address outlined in the SORN.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

Describe the potential risks associated with potentially insufficient notice and what steps, if any, are currently being taken to mitigate those identified risks. (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: There is a risk that workforce users who provide information to Saviynt will not know how their information is being stored or used in Saviynt.

Mitigation: The information provided will only be used for the purposes stated, and communication will be through multiple channels. Notice is published within the Privacy Act, PIA, and SORN.

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.***

Individuals may request access to Privacy Act records maintained by requesting a copy using the procedures defined at https://department.va.gov/foia/. 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 VA system of records, the facility Privacy Officer, or their designee.

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 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?

The system is a Privacy Act system.

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.

Individuals have the right to amend their records by submitting their request in writing. The request must be in writing and adequately describe the specific information the individual believes to be inaccurate, incomplete, irrelevant, or untimely and the reason for this belief. The written request needs to be mailed or delivered to the VA organization that maintains the record.

Information about VA records and contact information can be found at https://www.va.gov/records/. A request for amendment of information contained in a system of records must be delivered to the System Manager, or designee, for the concerned VA system of records, and the facility Privacy Officer, or designee.

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.

If an individual has questions pertaining to data submitted to the VA to obtain services, they will follow standard Amendment processes listed within the SORN and this PIA.

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 system will allow users to enter correct information and request access to authorized VA applications/systems.

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 an individual is unaware that their information is being collected by the system

- Individuals may not be able to access the correct resources needed for their role.
- Access reviews and audits may be based on incomplete and inaccurate information of the relevant employees whose access needs to be reviewed.

Mitigation: Individuals are provided notice of how to access, redress and correct information maintained in a VA system of record within the applicable SORN and the PIA. Any inaccuracies will be addressed immediately by users either making changes to the information that was entered or by others with the authority to make those corrections (such as HR, supervisors, or a ServiceNow support) on behalf of the individual.

As part of our process to onboard and implement new applications to Saviynt, data quality analysis will be a standard part of our integration process to ensure data accuracy before the data is transmitted into Saviynt.

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?

VA users gain access to the system through Single Sign-On with EntraID.

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?

Users from other government agencies do not have access to the system.

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.

There are standard user role types and their abilities to edit may depend on the role. There is a set of standard SAV roles that are used to control access within Saviynt. The intent is to build roles (enterprise and application-based roles) that grant access based on a user's role in the organization. These roles are used to push entitlements out to target systems. For example, there are:

Edit Access: Users, Managers, Admins, and SOD Auditors.
Read-Only Access: Read-Only Auditors and Technical Support roles.

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?

Contractors will be given access to hosting environment and complete their contractual obligations for ensuring the architecture and software are available and that it complies with VA OI&T policy. Contractors will have access to PII or data contained in the system in order to support integration of applications, implementation of access campaigns, and automate processes. Contractors are required to sign VA National Rules of Behavior (ROB) and/or Non-Disclosure Agreements (NDA) as required under contract stipulations.

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

Contractors will be given access to hosting environment and complete their contractual obligations for ensuring the architecture and software are available and that it complies with VA OI&T policy. Contractors will have access to PII or data contained in the system.

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

Contractors are a part of our delivery team to implement and stand up this tool, configure and integrate additional applications, and support its ATO achievement and maintenance.

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.

No additional privacy or security training would be offered specific to the Saviynt application. Existing VA privacy and PII trainings are deemed to be sufficient. VA awareness training program commences with the VA OIT TMS training, *VA Privacy and Information Security Awareness and Rules of Behavior (ROB), number 10176.* Following the training, all information system users will be able to identify the types of information that must be carefully handled to protect privacy; recognize the required information security practices, legal requirements, and consequences and penalties for non-compliance; and explain how to report incidents. The awareness program is consistent, updated and deployed for all employees regularly.

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

No

8.4a If completed, provide:

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

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.***

VA Sponsored FedRAMP ATO process is the initial A&A process for the Saviynt SaaS application and is In Process. The following items are included in this process: Security Plan, Authorization, and Risk Review. The estimated IOC date is 06/02/2025. The system is currently classified as Moderate Impact.

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)***

Saviynt is hosted in a single account AWS Gov Cloud (US), managed by Saviynt, since they are the SaaS vendor. This makes AWS Gov Cloud (US) the Cloud Service Provider (CSP). AWS GovCloud (US) allows the flexibility to architect secure cloud solutions that comply with the FedRAMP High baseline. AWS GovCloud (US) consists of 2 isolated AWS Regions (US-East and US-West) to allow an HA (Highly Available) solution in thee cloud while addressing specific regulatory and compliance requirements, including Federal Risk and Authorization Management Program (FedRAMP) High, Department of Defense Security Requirements Guide (DoD SRG) Impact Levels 2, 4 and 5, IRS-1075; and other compliance regimes. AWS GovCloud (US) Regions are logically and physically administered exclusively by AWS personnel that are U.S. citizens only. As a CSP, AWS follows the FedRAMP process to get their services authorized for Federal or DoD use. The FedRAMP process does not issue an Authority to Operate (ATO) to CSPs, instead, the FedRAMP process issues Provisional Authority to Operate (PATO). The PATO is a pre-procurement approval for Federal Agencies or the DoD to use AWS Gov Cloud (US).

This system is a Software as a Service (SaaS) through AWS Gov Cloud. The system is currently FedRAMP Authorized and active on the FedRAMP Marketplace under FedRAMP ID FR1821062403.

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.*

There is no contractual agreement between the VA and the CSP, AWS Gov Cloud. The agreement is between the VA and the SaaS solution vendor, “Saviynt”. However, the contract between the VA and the SaaS vendor states that all data within the SaaS solution is the exclusive property of the VA and that it may not be utilized in any form without specific permission from the VA. The contract identifier is NNG15SE09B.

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. Data collected is used solely for the purposes of providing Saviynt services and is protected through strict security measures.

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.

For information systems that are hosted, operated, maintained, or used on behalf of VA at non-VA facilities, Contractors/Subcontractors are fully responsible and accountable for ensuring compliance with all HIPAA, Privacy Act, FISMA, NIST, FIPS, and VA security and privacy directives and handbooks. This includes conducting compliant risk assessments, routine vulnerability scanning, system patching and change management procedures, and the completion of an acceptable contingency plan for each system. The Contractor's security control procedures must be equivalent to those procedures used to secure VA systems. A Privacy Impact Assessment (PIA) must also be provided to the COR and approved by VA Privacy Service prior to operational approval. All external Internet connections to VA network involving VA information must be in accordance with the TIC Reference Architecture and reviewed and approved by VA prior to implementation. For Cloud Services hosting, the Contractor shall also ensure compliance with the Federal Risk and Authorization Management Program (FedRAMP).

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).

The system does not use 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.

GINA SIEFERT Digitally signed by GINA SIEFERT
Date: 2025.05.14 09:05:25 -05'00'

Privacy Officer, Gina Siefert

JOHN DELEO Digitally signed by JOHN DELEO
Date: 2025.05.14 10:15:35 -04'00'

Information System Security Officer, Martin DeLeo

CHINO WALTERS Digitally signed by CHINO WALTERS
Date: 2025.05.14 10:35:56 -04'00'

Information System Owner, Chino Walters

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).

From the Declaration for Federal Employment, OMB No. 3206-0182:

Privacy Act Statement

The Office of Personnel Management is authorized to request this information under sections 1302, 3301, 3304, 3328, and 8716 of title 5, U. S. Code. Section 1104 of title 5 allows the Office of Personnel Management to delegate personnel management functions to other Federal agencies. If necessary, and usually in conjunction with another form or forms, this form may be used in conducting an investigation to determine your suitability or your ability to hold a security clearance, and it may be disclosed to authorized officials making similar, subsequent determinations. Your Social Security Number (SSN) is needed to keep our records accurate, because other people may have the same name and birth date. Public Law 104-134 (April 26, 1996) asks Federal agencies to use this number to help identify individuals in agency records. Giving us your SSN or any other information is voluntary. However, if you do not give us your SSN or any other information requested, we cannot process your application. Incomplete addresses and ZIP Codes may also slow processing. ROUTINE USES: Any disclosure of this record or information in this record is in accordance with routine uses found in System Notice OPM/GOVT-1, General Personnel Records. This system allows disclosure of information to: training facilities; organizations deciding claims for retirement, insurance, unemployment, or health benefits; officials in litigation or administrative proceedings where the Government is a party; law enforcement agencies concerning a violation of law or regulation; Federal agencies for statistical reports and studies; officials of labor organizations recognized by law in connection with representation of employees; Federal agencies or other sources requesting information for Federal agencies in connection with hiring or retaining, security clearance, security or suitability investigations, classifying jobs, contracting, or issuing licenses, grants, or other benefits; public and private organizations, including news media, which grant or publicize employee recognitions and awards; the Merit Systems Protection Board, the Office of Special Counsel, the Equal Employment Opportunity Commission, the Federal Labor Relations Authority, the National Archives and Records Administration, and Congressional offices in connection with their official functions; prospective non-Federal employers concerning tenure of employment, civil service status, length of service, and the date and nature of action for separation as shown on the SF 50 (or authorized exception) of a specifically identified individual; requesting organizations or individuals concerning the home address and other relevant information on those who might have contracted an illness or been exposed to a health hazard; authorized Federal and non-Federal agencies for use in computer matching; spouses or dependent children asking whether the employee has changed from a self-and-family to a self-only health benefits enrollment; individuals working on a contract, service, grant, cooperative agreement, or job for the Federal government; non-agency members of an agency's

performance or other panel; and agency-appointed representatives of employees concerning information issued to the employees about fitness-for-duty or agency-filed disability retirement procedures.

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)

Guidelines on Security and Privacy in Cloud Computing – NIST
https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-144.pdf

AWS NIST Compliance Reference
https://aws.amazon.com/compliance/nist/