Privacy Impact Assessment for the VA IT System called:

ServiceNow External Application Support Environment (ServiceNow Support)

Veterans Affairs Central Office (VACO)

Office of Information Technology, Infrastructure Operations

eMASS ID # 2394

Date PIA submitted for review:

May 9, 2024

System Contacts:

System Contacts

Title	**Name**	**E-mail**	**Phone Number**
Privacy Officer	Gina Siefert	Gina.siefert@va.gov and oitprivacy@va.gov	Office: 202-632-8430
Information System Security Officer (ISSO)	Yentl Brooks	Yentl.Brooks@va.gov	Office: 713-383-1879
Information System Owner (ISO)	Prashanthi Kuchikulla	Prashanthi.Kuchikulla@va.gov	Office: 202-277-9536

Abstract

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

The ServiceNow External Application Support Environment (acronym name is ServiceNow Support) is a Red Hat OpenShift cluster supporting ServiceNow. The ServiceNow Support environment will host a containerized middle-tier application facilitating the extraction of data from ServiceNow for short-term storage on a data bus and relayed for longer-term storage to an external data lake or database. This will improve ServiceNow Support platform performance by enabling more efficient reporting and further analysis of ServiceNow Support data across the VA without impacting the responsiveness of performance of the ServiceNow application.

Overview

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

1 General Description

A. What is the IT system name and the name of the program office that owns the IT system?

The official VA registered system name is ServiceNow External Application Support Environment, (acronym name is ServiceNow Support) owned by the Office of Information Technology (OIT) – Infrastructure Operations (IO) – Enterprise Service Management (ESM).

B. What is the business purpose of the program, IT system, or technology and how it relates to the program office and agency mission?

The official VA registered system name is ServiceNow External Application Support Environment, and the system acronym is "ServiceNow Support," both of which are shown in Enterprise Mission Assurance Support Service (eMASS). The software that supports VA Operations enterprise-wide is ServiceNow and is referenced throughout all system documents as the IT system. That software supports VA Operations enterprise-wide ServiceNow External Application Support Environment (ServiceNow Support) is a Red Hat OpenShift cluster supporting ServiceNow. The ServiceNow Support environment will host a containerized middle-tier application facilitating the extraction of data from the ServiceNow system for short-term storage on a data bus and relayed for longer-term storage to an external data lake or database. This will improve the ServiceNow system platform performance by enabling more efficient reporting and further analysis of ServiceNow data across the VA without impacting the responsiveness of performance of the ServiceNow application.

C. Who is the owner or control of the IT system or project?

This IT system is Veterans Affairs (VA) owned and operated.

2. Information Collection and Sharing

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

ServiceNow Support will have approximately 100 users of this system. These 100 users will be the VA employees and contractors in the OIT organization. No one outside of OIT will have any access to ServiceNow Support.

The total number of individuals of information stored is 2,000,000. This number includes VA employees, contractors, and Veterans.

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

ServiceNow Support is designed to provide short-term storage of all the ServiceNow (GCC-E) system data and will enable efficient report and data analysis in near real-time. ServiceNow Support will transfer all data to the Summit Data Platform's Data Lake for longer-term storage, analysis, reporting, and use by authorized VA users.

All data within Service Now Support system is collected through the ServiceNow (GCC-E) system. For the purposes of this PIA, Service Now (GCC-E) is considered to be a secondary system (source system) to ServiceNow Support.

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

VA Platform One (VAPO) system maintains the underlying physical infrastructure for ServiceNow Support and maintains connections with ServiceNow (GCC-E) system, Red Hat Active Message Queue (AMQ) and AMQ Streams (Kafka Bus), all within the VA boundary (VA.GOV).

G. Is the system is operated in more than one site, and if so, a description of how use of the system and PII is maintained consistently in all sites and if the same controls are used across sites?

ServiceNow Support is maintained in a primary data center with an alternate data facility. It operates in compliance with privacy controls applicable to systems with Personally Identifying Information (PII) and Protected Health Information (PHI) being stored, transmitted, and processed. Privacy controls are documented in the ServiceNow Support System Security Plan (SSP). Controls are also enacted for ServiceNow Support in accordance with HIPAA Business Associate Agreement (BAA) policies and procedures. ServiceNow Support handles and retains system information in accordance with applicable federal laws, executive orders, directives, policies, regulations, standards, and operational requirements. The release of privacy-related data by accident or malicious intent would have zero, minor or moderate effects, based on protection controls such as those dealing with authentication, encryption, and firewall mechanisms.

3. Legal Authority and SORN

H. What is the citation of the legal authority to operate the IT system?

The following is a full list of related laws, regulations, policies, and the legal authorities:

- Title 45 Code of Federal Regulations (C.F.R.) Subtitle A, Subchapter C, Part 164, Subpart E "Privacy of Individually Identifiable Health Information:
- Confidentiality of Certain Medical Records, Title 38 U.S.C. § 7332
- E-Government Act of 2022 (44 U.S.C. § 208(b))
- Federal Information Security Management Act (FISMA) of 2002
- Health Insurance Portability and Accountability Act (HIPAA) Security Rule, Title 45 C.F.R. Part 160
- Information Technology Management Reform Act of 1996 (also known as the Clinger - Cohen Act)
- NIST 800-47, Security Guide for Interconnecting Information Technology Systems
- OMB Circular A-130, Managing Information as a Strategic Resource
- OMB Circular A-130, Appendix III, "Security of Federal Automated Information Systems"
- OMB M-03-22, "OMB Guidance for Implementing the Privacy Provisions of the E- Government Act of 2002
- Privacy Act of 1974, 5 U.S.C. § 552a, as amended
- System of Record Notice (SORN) –
  17VA26 / 88 FR 44462 - Loan Guarantee Fee Personnel and Program Participant Records-VA
- System of Record Notice (SORN) –
  27VA047 / 77 FR 39346 - Personnel & Acct Integrated Data system
- System of Record Notice (SORN) –
  55VA26 / 88FR 63686 - Loan Guaranty Home, Condominium and Manufactured Home Loan Applicants Records
- System of Record Notice (SORN) – 168VA005 / 86 FR 6975 - Health Information Exchange
- System Record Notice (SORN) –
  24VA10A7 / 85 FR 62406 - Patient Medical Records-VA
- System of Record Notice (SORN) –
  146VA005Q3 / 73 FR 16093 – Department of Veterans Affairs Identity Management System (VAIDMS)-VA
- Title 18 U.S.C. § 641 Criminal Code: "Public Money, Property or Records"
- Title 18 U.S.C. § 1905 Criminal Code: "Disclosure of Confidential Information"
- Title 38, United States Code (U.S.C), § 501(a), § 1705, § 1710, § 1722, and § 5317
- Title 38 United States Code (U.S.C.) §§ 5721-5728, "Veteran's Benefits, Information Security"
- Title 5 U.S.C. § 552 and § 552a
- Title 5 U.S.C. § 11001, "Enhanced Personnel Security Programs"
- VA Directive 6500: VA Cybersecurity Program
- VA Directive 6502, VA Enterprise Privacy Program
- VA Privacy Threshold Analysis and Privacy Impact Assessment Informational Guide (FY 23 PTA and PIA Guide.docx), published at PIA Training Resources - PIA Training Resources (sharepoint.com)
- VA Directive and Handbook 6513, *Secure External Connections*
- Title 38 U.S.C § 5701: Confidential Nature of Claims

See VA Handbook 6500.6, Appendix C and D.

I. If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval? If the system is using cloud technology, does the SORN for the system cover cloud usage or storage?

No, ServiceNow Support does not create a System of Record of Notice (SORN). VA ServiceNow Support is not a System of Record (SOR), nor does it generate records, only an incident record to track various listed requests. ServiceNow Support does utilize sources from within the VA for information to validate, sort, approve and complete official VA business.

4. System Changes

J. Will the completion of this PIA will result in circumstances that require changes to business processes?

No, the completion of this PIA will not require changes to business processes but will help manage the VA business processes more accurately and efficiently.

K. Will the completion of this PIA could potentially result in technology changes?

No, the completion of this PIA will not potentially result in technology changes to business processes but will help manage the VA business processes more accurately and efficiently.

Section 1. Characterization of the Information

The following questions are intended to define the scope of the information requested and collected as well as the reasons for its collection as part of the program, IT system, or technology being developed.

1.1 What information is collected, used, disseminated, created, or maintained in the system?

Identify and list all Sensitive Personal Information (SPI) that is collected and stored in the system, including Individually Identifiable Information (III), Individually Identifiable Health Information (IIHI), Protected Health Information (PHI), and Privacy- Protected Information. For additional information on these information types and definitions, please see VA Directives and Handbooks in the 6500 series (https://vaww.va.gov/vapubs/). If the system creates information (for example, a score, analysis, or report), list the information the system is responsible for creating.

If a requesting system receives information from another system, such as a response to a background check, describe what information is returned to the requesting system.
This question is related to privacy control AP-1, Authority to Collect, and AP-2, Purpose Specification.

The information selected below must match the information provided in question 2.1 as well as the data elements columns in 4.1 and 5.1. 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	☒ Personal Mailing Address	☐ Personal Fax Number
☒ Social Security Number	☒ Personal Phone Number(s)	☒ Personal Email Address
☒ Date of Birth		☒ Emergency Contact Information (Name, Phone
☐ Mother's Maiden Name		

Number, etc. of a different individual)
☒ Financial Information
☒ Health Insurance Beneficiary Numbers Account numbers
☐ Certificate/License numbers[1]
☐ Vehicle License Plate Number

☐ Internet Protocol (IP) Address Numbers
☒ Medications
☒ Medical Records
☒ Race/Ethnicity
☒ Tax Identification Number
☒ Medical Record Number
☒ Gender

☒ Integrated Control Number (ICN)
☒ Military History/Service Connection
☒ Next of Kin
☒ Other Data Elements (list below)

Other PII/PHI data elements:

Electronic Data Interchange Personal Identifier (EDIPI)
Employee Identification Number (EIN
Employee Record Number (ERN)
Internal Control Number (ICN
Personal Identity Verification (PIV) Identification (ID
Property Physical Address (Veteran
Security Identification (SecID)
Vendor Taxpayer ID Number (TIN

PII Mapping of Components (Servers/Database)

ServiceNow Support consists of 2 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 ServiceNow Support 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 3.9 in the PTA should be used to answer this question.

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

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
Red Hat Active Message Queue (AMQ)	Yes	Yes	Date of Birth (DOB), Electronic Data Interchange-Personal Identifier (EDIPI) Employee Identification Number (EIN), Employee Record Number (ERN), Financial Information (Veteran), Financial Information (VA), Full Legal Name, Gender, Integration Control Number (ICN), Medical Records, Military History/Service, Patient ID, Personal Email Address, Personal Identity Verification (PIV) ID, Personal Mailing Address, Personal Phone Number, Race/Ethnicity, Security Identification Number (SecID), Social Security Number (SSN), Vendor Taxpayer ID Number (TIN)	Associated identification data to ensure accuracy of incident tracking for Official VA business purposes	TLS 1.2; Security Controls in place, FedRAMP certified
AMQ Streams (Kafka Bus)	Yes	Yes	Date of Birth (DOB), Electronic Data Interchange-Personal Identifier (EDIPI) Employee Identification Number (EIN), Employee	Associated identification data to ensure accuracy of incident	TLS 1.2; Security Controls in place, FedRAMP certified

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
			Record Number (ERN), Financial Information (Veteran), Financial Information (VA), Full Legal Name, Gender, Integration Control Number (ICN), Medical Records, Military History/Service, Patient ID, Personal Email Address, Personal Identity Verification (PIV) ID, Personal Mailing Address, Personal Phone Number, Race/Ethnicity, Security Identification Number (SecID), Social Security Number (SSN), Vendor Taxpayer ID Number (TIN)	tracking for Official VA business purposes	

1.2 What are 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?

All data within ServiceNow Support is collected from ServiceNow (GCC-E) records.

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 ServiceNow External Application Support Environment (ServiceNow Support) is a Red Hat OpenShift cluster supporting the ServiceNow (GCC-E) system. The ServiceNow Support environment will host a containerized middle-tier application facilitating the extraction of data from ServiceNow (GCC-E) system for short-term storage on a data bus and relayed for longer-term storage to an external data lake or database. This will improve ServiceNow platform performance by enabling more efficient reporting and further analysis of ServiceNow data across the VA without impacting the responsiveness of performance of the ServiceNow application. The data in ServiceNow Support is collected from the ServiceNow (GCC-E) system records for VA reporting and data analysis.

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

VA ServiceNow Support does not create information using scores, analyses, and reports. This data is available in ServiceNow Support and may be exported to approved systems for additional or further analysis and reporting.

1.3 How is the information collected?

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?

ServiceNow Support receives information from the direct integration with ServiceNow (GCC-E) system.

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?

ServiceNow Support information is not collected on a form and is not subject to the Paperwork Reduction Act.

1.4 How will the information be checked for accuracy? 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.

ServiceNow (GCC-E) system is the source record for VA Incident Management (Mgmt.). This supports reporting and dashboarding across the VA by supplying data for Incident Mgmt., Change Mgmt., Problem Mgmt., and Project Mgmt.

ServiceNow Support data is not checked for accuracy, but is imported from ServiceNow (GCC-E) for further analysis and reporting by users across the VA. The purpose of the information collected, used, and created by ServiceNow Support is to create unique records for each user that is validated through Identity and Access Management (IAM). This SPI is used to associate an end user within ServiceNow (GCC-E) system with additional workflow capabilities such as incident management, problem management, demand management, change management and asset management. The SPI collected and used within ServiceNow Support is critical to meeting the Infrastructure Operations (IO) mission as a customer-centric organization focused in efficiently delivering secure and high availability infrastructure solutions in support of VA's mission and to collaborate with our business partners to create the best experience for all Veterans. All SPI/PII/PHI is encrypted while in transit and at rest via Hypertext Transfer Protocol Secure (HTTPS).

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?

ServiceNow Support does not use a commercial aggregator to check for accuracy.

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

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

ServiceNow Support derives authority from ServiceNow (GCC-E) system:

- Title 38 Code of Federal Regulations (CFR) provides the legal authority that permits the collection of personally identifiable information (PII). VA Directive 6502, VA Enterprise Privacy Program (5 May2008) provides the legal authority that permits use, maintenance, and sharing of personally identifiable information (PII), either generally or in support of a specific program or information system need.

- Before collecting PII for the ServiceNow Support system, the Privacy Officer (PO), Information System Security Officer (ISSO), and / or Information System Owner (ISO) determine whether the contemplated collection, use, maintenance, and sharing of PII is legally authorized for use in a specific program or information system. The authority to collect, use, maintain, and share PII is documented in the System of Records Notice (SORN) and/or Privacy Threshold Analysis, (PTA) and/or Privacy Impact Assessment (PIA) or other applicable documentation such as Privacy Act Statements.

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

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

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

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

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

Principle of Data Quality and Integrity: Are there policies and procedures for VA to ensure that personally identifiable information is accurate, complete, and current?
This question is related to privacy control AR-1, Governance and Privacy Program, and AR-2, Privacy Impact and Risk Assessment.

Follow the format below when entering your risk assessment:

Privacy Risk:

1. Sensitive Personal Information (SPI), including personal contact information, SSN/TIN, may be released to unauthorized individuals.
2. Sensitive Personal Information (SPI), including personal contact information, SSN/TIN, may be released to unauthorized individuals.
3. Unsecured Sensitive Personal Information (SPI), including personal contact information, SSN/TIN, may be exposed.
4. Data breach at the network level.

Mitigation:

1. Profile based permissions will govern what access users have to the system. Profiles, including groups and roles within ServiceNow Support, is reviewed on a regular basis by the VA IO ServiceNow Platform Owners (Sr. FTE) to ensure that appropriate information is shared with appropriate users. All employees with access to VA information systems are required to complete the "VA Privacy, Information Security Awareness Training and Rules of Behavior" annually.
2. Profile based permissions will govern what access users have to the system. Profiles, including groups and roles within ServiceNow Support, is reviewed on a regular basis by the VA IO ServiceNow Platform Owners (Sr. FTE) to ensure that appropriate information is shared with appropriate users. All employees with access to VA information systems are required to complete the "VA Privacy, Information Security Awareness Training and Rules of Behavior" annually.
3. To ensure the utmost privacy and security at the facility level, authorized personnel must pass through multiple levels of physical and administrative controls to access the ServiceNow system. All buildings are completely anonymous, with bullet-resistant exterior walls, and embassy-grade concrete posts and planters around the perimeter. All exterior entrances feature silent alarm system that notify law enforcement in the event of a suspected intrusion. Data is backed up. Backups do no not physically leave the data center.

4. Multilevel security products from leading security vendors and proven security practices ensure network security. To prevent malicious attacks through unmonitored ports, external firewalls allow only https traffic on ports 80 and 443, along with Internet Control Message Protocol (ICMP) traffic. Switches ensure that the network complies with the Request for Comment (RFC) 1918 standard, and address translation technologies further enhance network security. Intrusion Detection Sensors (IDS) protect all network segments. Internal software systems are protected by two-factor authentication, along with the extensive use of technology that controls points of entry.

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
Date of Birth (DoB)	File/Record Identification purposes	Not used
Electronic Data Interchange-Personal Identifier (EDIPI)	File/Record Identification purposes; Used to validate active Department of Defense Common Access Card (CAC) holders accessing VA IT systems	Not used
Employee Identification Number (EIN)	File/Record Identification purposes; VA Employee Identification number created when HR performed an integration from data dictionary terms and is still used as a tracker	Not used
Employee Record Number (ERN)	File/Record Identification purposes; A number to identify civilian employees	Not used
Financial Information	File/Record Identification purposes	Not used
Full Legal Name	File/Record Identification purposes	Not used
Gender	File/Record Identification purposes	Not used
Health Insurance Information	File/Record Identification purposes	Not used
Integration Control Number (ICN)	File/Record Identification purposes; Includes the 17 alpha-numeric (10 digits + "V" + 6 digits) VA-assigned internal control number (ICN) in the insured's I.D. field. Veteran's ICN can be found on the VA issued HSRM referral. The Veteran's full 9-digit social security number (SSN) may be used if the ICN is not available.	Not used

Medical Records (includes Medications)	File/Record Identification purposes	Not used
Military History / Service	File/Record Identification purposes	Not used
Next of Kin Information	File/Record Identification purposes	Not used
Patient ID	File/Record Identification purposes	Not used
Personal & Cellular Phone Number	File/Record Identification purposes	Not used
Personal Email Address	File/Record Identification purposes	Not used
Personal Identity Verification (PIV) ID	File/Record Identification purposes; Used to validate the identity of VA system users	Not used
Personal Mailing Address	File/Record Identification purposes	Not used
Property Physical Address (Veteran)	File/Record Identification purposes; Used if different from the regular mailing address used for Veteran home loan process (LGY)	Not used
Race/Ethnicity	File/Record Identification purposes	Not used
Security Identification (SecID)	File/Record Identification purposes; VA Employee Identification number	Not used
Social Security Number (SSN)	File/Record Identification purposes	Not used
Security Identification Number (SecID)	File/Record Identification purposes	Not used
Vendor Taxpayer ID Number (TIN) (Financial information)	File/Record Identification purposes; Tax identification number used by contractors	Not used

2.2 What types of tools are 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?

ServiceNow (GCC-E) system is the source record for VA Incident Management (Mgmt.). This supports reporting and dashboarding across the VA by supplying data for Incident Mgmt., Change Mgmt., Problem Mgmt., and Project Mgmt.

ServiceNow Support receives, creates, and stores data. ServiceNow Support does contain performance analytics functions that will enable users to perform data analysis, queries and custom searches for VA support.

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.

No, ServiceNow Support does not create or make available previously unused information.

2.3 How is the information in the system 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 is encrypted while in transit and at rest via Hypertext Transfer Protocol Secure (HTTPS).

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

ServiceNow External Application Support Environment leverages FIPS 140-2 validated cryptographic modules wherever encryption is required; cryptographic modules are implemented in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.

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

In accordance with OMB Memorandum M-06-15, all SPI/PII/PHI is encrypted while in transit and at rest via Hypertext Transfer Protocol Secure (HTTPS). The Confidentiality, Integrity, and Assessment (CIA) rating for VA ServiceNow Support is impact rated a "High," which includes additional precautions used for the system to be properly secured within the VA cloud boundary in VA Platform One (VAPO). The Uniform Resource Locator (URL) is encrypted via https.

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?

ServiceNow Support will have approximately 100 users of this system. These 100 users will be the VA employees and contractors in the OIT organization. No one outside of OIT will have any access to ServiceNow Support. The access to ServiceNow Support is granted by a role-based need to access this system and is limited. VA managers/supervisors provide approval for access to ServiceNow Support. The VA Enterprise will not have access to ServiceNow Support.

Safeguards are implemented to ensure data is not sent to unauthorized VA employees, including employee privacy and security training, and required reporting of suspicious activity. The principle of need-to-know is strictly adhered to by ServiceNow Support; and this is enforced by ServiceNow Support best practices of assigning users to groups and roles based on job functions.

2.4b Are criteria, procedures, controls, and responsibilities regarding access documented?

Access is documented. Reference, KB0113920 - ServiceNow: Assignment Group Standardization Guide (https://yourit.va.gov/va?sys_kb_id=2382c9891b9eddd0d73ccb78624bcbcd&id=kb_article_view&sysparm_rank=3&sysparm_tsqueryId=1c069a068794ad906d08642d3fbb357f) .

2.4c Does access require manager approval?

Yes, VA managers/supervisors provide approval for access to ServiceNow Support. The use of groups and roles within ServiceNow Support limits the amount of data a user may access. In accordance with ServiceNow best practices, users are assigned to groups, and groups inherit roles based on assigned groups. Reference, KB0113920 - ServiceNow: Assignment Group Standardization Guide (https://yourit.va.gov/va?sys_kb_id=2382c9891b9eddd0d73ccb78624bcbcd&id=kb_article_view&sysparm_rank=3&sysparm_tsqueryId=1c069a068794ad906d08642d3fbb357f).

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

Yes, VA managers/supervisors provide approval for access to ServiceNow Support. The use of groups and roles within ServiceNow Support limits the amount of data a user may access. PII is not visible to all users, the name and SSN/file number of veterans experiencing problems with Veterans Benefit Management System (VBMS) is stored in protected fields for VBMS use only. In accordance with ServiceNow Support best practices, users are assigned to groups, and groups inherit roles based on assigned groups. Reference, KB0113920 - ServiceNow: Assignment Group Standardization Guide (https://yourit.va.gov/va?sys_kb_id=2382c9891b9eddd0d73ccb78624bcbcd&id=kb_article_view&sysparm_rank=3&sysparm_tsqueryId=1c069a068794ad906d08642d3fbb357f).

2.4e Who is responsible for assuring safeguards for the PII?

The Information System Owner (ISO) is responsible for assuring safeguards for PII. The Uniform Resource Locator (URL) is encrypted via Hypertext Transfer Protocol Secure (HTTPS).

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*

Date of Birth (DoB)
Electronic Data Interchange-Personal Identifier (EDIPI)
Employee Identification Number (EIN)
Employee Record Number (ERN)
Financial Information
Full Legal Name
Gender
Health Insurance Info
Integration Control Number (ICN)
Medical Records (includes medications)
Military History/Service
Next of Kin Information
Patient ID
Personal Email Address
Personal Identity Verification (PIV) ID
Personal Mailing Address
Personal Phone Number
Property Physical Address (Veteran)
Race/Ethnicity
Security Identification Number (SecID)
Social Security Number (SSN)
Vendor Taxpayer ID Number (TIN) (Financial information)

3.2 How long is information retained?

*In some cases, VA may choose to retain files in active status and archive them after a certain period of time. State active file retention periods, as well as archived records, in number of years, for the information and record types. For example, financial data held within your system may have a different retention period than medical records or education records held within your system, please be sure to list each of these retention periods. **The VA records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented.** If the system is using cloud technology, will it be following the NARA approved retention length and schedule? This question is related to privacy control DM-2, Data Retention and Disposal.*

Information within ServiceNow Support has been classified to contain three types of information: Help Desk Services, Lifecycle/Change Management, System and Network Monitoring.

Help Desk Services: Record Control Schedule (RCS) 5.8-010. Technical and administrative help desk operational records (https://www.archives.gov/files/records-

mgmt/grs/grs05-8.pdf). Data retention and disposition classification: Temporary; destroy 1 year after resolved, or when no longer needed for business use, whichever is appropriate. DAA-GRS-2017-0001-0001 (https://www.archives.gov/files/records-mgmt/rcs/schedules/general-records-schedules/daa-grs- 2017-0003_sf115.pdf).

Lifecycle/Change Management: RCS 3.1-030. Configuration and Change Management Records (https://www.archives.gov/records-mgmt/grs/grs03-1.pdf). Data retention and disposition classification: Temporary; destroy 5 years after system is superseded by a new iteration, or is terminated, defunded, or no longer needed for agency/IT administrative purposes, but longer retention is authorized if required for business use. DAA-GRS-2013-0005-0005 (https://www.archives.gov/files/records-mgmt/rcs/schedules/general-records-schedules/daa-grs- 2013-0005_sf115.pdf

System and Network Monitoring: RCS 3.1-020. Information technology operations and maintenance records (https://www.archives.gov/records-mgmt/grs/grs03-1.pdf). Data retention and disposition classification: Temporary; destroy 3 years after agreement, control measures, procedures, project, activity, or transaction is obsolete, completed, terminated or superseded, but longer retention is authorized if required for business use.DAA-GRS-2013-0005-0004 (https://www.archives.gov/files/records-mgmt/rcs/schedules/general-records-schedules/daa-grs- 2013-0005_sf115.pdf).

3.3 Has the retention schedule been 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. The schedule must be formally offered to NARA for official approval. Once NARA approves the proposed schedule, the VA records officer will notify the system owner. Please work with the system Privacy Officer and 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. The ServiceNow Support retention schedule is compliant with VA Directive 6300, Records and Information Management (https://vaww.va.gov/vapubs/viewPublication.asp?Pub_ID=997&FType=2), and National Archives Federal Records Management policies (http://www.ecfr.gov/cgi-bin/text-idx?SID=28eaaab268f0dd47e9fb9b4f87e9445a&tpl=/ecfrbrowse/Title36/36CXIIsubchapB.tpl).

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

Yes. The ServiceNow Support retention schedule is compliant with VA Directive 6300, Records and Information Management (https://vaww.va.gov/vapubs/viewPublication.asp?Pub_ID=997&FType=2), and National Archives Federal Records Management policies (http://www.ecfr.gov/cgi-bin/text-idx?SID=28eaaab268f0dd47e9fb9b4f87e9445a&tpl=/ecfrbrowse/Title36/36CXIIsubchapB.tpl).

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

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

Electronic data and files of any type, including Protected Health Information (PHI), Sensitive Personal Information (SPI), Human Resources records, and more are destroyed in accordance with the Department of Veterans Affairs Directive 6500, VA Cybersecurity Program, (24 February 2021), (https://vaww.va.gov/vapubs/viewPublication.asp?Pub_ID=1003&FType=2).

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.

ServiceNow Support has a development environment that is a clone of the production environment. PII is carried over to ensure accuracy and thoroughness in the test and development of new features and capabilities in ServiceNow Support. Access to these environments is managed by the Manager, Service Management Platforms and Tools (SMPT) Implementation.

Development Environment: 517,000 records; access: Single Sign-On (SSO). This environment is primarily used by developers, approximately 10 users.

Production Environment: 517,000 records; access: Single Sign-On (SSO). This is the Production Environment. Approximately 90 users.

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 ISSO to complete all Privacy Risk questions inside the document this section).

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

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

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

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

Follow the format below:

Privacy Risk: The risk to maintaining data within ServiceNow Support is due to longer retention times increase the risk that information can be compromised or breached.

Mitigation: To mitigate the risk posed by information retention, ServiceNow Support adheres to the VA RCS schedules for each category or data it maintains. When the retention data is reached for a record, the ServiceNow Support team carefully disposes of the data by the determined method as described in question 3.4. All electronic storage media used to store, process, or access ServiceNow records will be disposed of in adherence with the latest version of VA Handbook 6500, Risk Management Framework for VA Information Systems VA Information Security Program.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

4.1 With which internal organizations is information shared/received/transmitted? What information is shared/received/transmitted, and for what purpose? How is the information transmitted?

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

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

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

For each interface with a system outside your program office, state what specific data elements (PII/PHI) are shared with the specific program office, contractor-supported IT system, and any other organization or IT system within VA.
Describe how the information is transmitted. For example, is the information transmitted electronically, by paper, or by some other means? Is the information shared in bulk, on a case-by-case basis, or does the sharing partner have direct access to the information?
This question is related to privacy controls AP-2, Purpose Specification, AR-3, Privacy Requirements for Contractors and Service Providers, AR-8, Accounting of Disclosures, TR-1, Privacy Notice, and UL-1, Internal Use.

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system***	***Describe the method of transmittal***
Government Community Cloud – Enterprise (GCC-E	Associated identification data to ensure accuracy of incident tracking for official VA business purposes	Date of Birth (DOB), Electronic Data Interchange-Personal Identifier (EDIPI), Employee Identification Number (EIN), Employee Record Number (ERN), Financial Information (Veteran), Financial Information (VA), Full Legal Name, Gender, Health Insurance Information, Integration Control Number (ICN), Medical Records, Military History/Service, Next of Kin Information, Patient ID, Personal Email Address, Personal Identity Verification (PIV) ID, Personal Mailing Address, Personal Phone Number, Race/Ethnicity, Security Identification Number (SecID), Social Security Number (SSN), Vendor Taxpayer ID Number (TIN)	Transport Layer Security (TLS) 1.2
Summit Data Platform (SD	Associated identification data to ensure accuracy of incident tracking for official VA business purposes	Date of Birth (DOB), Electronic Data Interchange-Personal Identifier (EDIPI), Employee Identification Number (EIN), Employee Record Number (ERN), Financial Information (Veteran), Financial Information (VA), Full Legal Name, Gender, Health Insurance Information, Integration Control Number (ICN), Medical Records, Military History/Service, Next of Kin Information, Patient ID, Personal Email Address, Personal Identity Verification (PIV) ID, Personal Mailing Address, Personal Phone Number, Race/Ethnicity, Security Identification Number (SecID), Social Security Number (SSN), Vendor Taxpayer ID Number (TIN)	Transport Layer Security (TLS) 1.2

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

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

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

Follow the format below:
Privacy Risk: There is a risk that information may be shared with unauthorized VA personnel.

Mitigation: Safeguards are implemented to ensure data is not sent to unauthorized VA employees, including employee privacy and security training, and required reporting of suspicious activity. The principle of need-to-know is strictly adhered to by ServiceNow Support, and this is enforced by approving access to the system's data based on business case for access and management approval.

Section 5. External Sharing/Receiving and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to VA, which includes Federal, State, and local governments, and the private sector.

5.1 With which external organizations (outside VA) is information shared/received? What information is shared/received, and for what purpose? How is the information transmitted and what measures are taken to ensure it is secure?

Is the sharing of information outside the agency compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If not, please describe under what legal mechanism the IT system is allowed to share the information in identifiable form or personally identifiable information outside of VA.

NOTE: Question 3.10 on Privacy Threshold Analysis should be used to answer this question.
Identify and list the names of any Federal, State, or local government agency or private sector organization with which information is shared.

For each interface with a system outside VA, state what specific data elements (PII/PHI) are shared with each specific partner.

What legal mechanisms, authoritative agreements, documentation, or policies are in place detailing the extent of the sharing and the duties of each party? For example, is the sharing of data compatible with your SORN? Then list the SORN and the applicable routine use from the SORN. Is there a Memorandum of Understanding (MOU), Computer Matching Agreement (CMA), or law that mandates the sharing of this information?

Describe how the information is transmitted to entities external to VA and what security measures have been taken to protect it during transmission.

This question is related to privacy control UL-2, Information Sharing with Third Parties

No. Data is not shared outside the VA.

Data Shared with External Organizations

List External Program Office or IT System information is shared/received with	***List the purpose of information being shared / received / transmitted with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program or IT system***	***List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)***	***List the method of transmission and the measures in place to secure data***
N/A				

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

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

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

Information contained within this system is not collected from individuals. All data within the Service Now Support system is collected through ServiceNow (GCC-E).

Notice before the collection of information is provided by various source systems with the publication of System of Record Notice (SORN) in the Federal Register and the publicly available Privacy Impact Assessment for the systems.

The following SORN's provide notice:

- 17VA26 / 78 FR 71727 - Loan Guarantee Fee Personnel and Program Participant Records-VA
- 27VA047 / 77 FR 39346 - Personnel & Acct Integrated Data system
- 55VA26 - Loan Guaranty Home, Condominium and Manufactured Home Loan Applicants Records
- 168VA005 / 86 FR 6975 - Health Information Exchange
- 24VA10A7 / 85 FR 62406 - Patient Medical Records-
- VA146VA005Q3 / 73 FR 16093 – Department of Veterans Affairs Identity Management System (VAIDMS)

6.1b If notice was not provided, explain why. If it was provided, attach a copy of the current notice.

Notice before the collection of information is provided by various source systems. The following SORN's provide notice:

- 17VA26 / 78 FR 71727 - Loan Guarantee Fee Personnel and Program Participant Records-VA
- 27VA047 / 77 FR 39346 - Personnel & Acct Integrated Data system
- 55VA26 - Loan Guaranty Home, Condominium and Manufactured Home Loan Applicants Records
- 168VA005 / 86 FR 6975 - Health Information Exchange
- 24VA10A7 / 85 FR 62406 - Patient Medical Records-
- VA146VA005Q3 / 73 FR 16093 – Department of Veterans Affairs Identity Management System (VAIDMS)

6.1c Describe how the notice provided for the collection of information is adequate to inform those affected by the system that their information has been collected and is being used appropriately. Provide information on any notice provided on forms or on Web sites associated with the collection.

Notice before the collection of information is provided by various source systems with the publication of System of Record Notices (SORN) in the Federal Register and the publicly available Privacy Impact Assessment for the system. The SORN explains the purpose of the system, the categories of individuals covered by the system, and how the information that is collected will be used.

The following SORN's provide this information:

- 17VA26 / 78 FR 71727 - Loan Guarantee Fee Personnel and Program Participant Records-VA
- 27VA047 / 77 FR 39346 - Personnel & Acct Integrated Data system
- 55VA26 - Loan Guaranty Home, Condominium and Manufactured Home Loan Applicants Records
- 168VA005 / 86 FR 6975 - Health Information Exchange
- 24VA10A7 / 85 FR 62406 - Patient Medical Records-
- VA146VA005Q3 / 73 FR 16093 – Department of Veterans Affairs Identity Management System (VAIDMS)

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.

The right to decline to provide information would be provided by the source system. Individuals communicating with the VA do have the opportunity and right to decline to provide information. However, failure to provide requested identifying information may cause the denial of services, based on the totality of circumstances for each situation. Individuals may communicate with the VA anonymously, and they may decline to provide additional identifying information at their discretion. These situations may also cause the denial of service or VA's inability to provide a response to anonymous correspondence. These situations are handled on a case-by-case basis. Information about individuals who correspond with VA is collected and stored in the source systems, as described in the various SORN. Both the SORN and Privacy Impact Assessment serve as public notice of these data collection policies. The following SORN's provide this information:

- 17VA26 / 78 FR 71727 - Loan Guarantee Fee Personnel and Program Participant Records-VA
- 27VA047 / 77 FR 39346 - Personnel & Acct Integrated Data system
- 55VA26 - Loan Guaranty Home, Condominium and Manufactured Home Loan Applicants Records
- 168VA005 / 86 FR 6975 - Health Information Exchange

- 24VA10A7 / 85 FR 62406 - Patient Medical Records-
- VA146VA005Q3 / 73 FR 16093 – Department of Veterans Affairs Identity Management System (VAIDMS)

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.

Yes, Individuals have a right to consent to particular uses of their information. Individuals voluntarily provide information when submitting correspondence or other documents to the Department. These processes are explained in the applicable source system SORN.

- 17VA26 / 78 FR 71727 - Loan Guarantee Fee Personnel and Program Participant Records-VA
- 27VA047 / 77 FR 39346 - Personnel & Acct Integrated Data system
- 55VA26 - Loan Guaranty Home, Condominium and Manufactured Home Loan Applicants Records
- 168VA005 / 86 FR 6975 - Health Information Exchange
- 24VA10A7 / 85 FR 62406 - Patient Medical Records-
- VA146VA005Q3 / 73 FR 16093 – Department of Veterans Affairs Identity Management System (VAIDMS)

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 System ISSO 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> Has sufficient notice been provided to the individual?

<u>Principle of Use Limitation:</u> Is the information used only for the purpose for which notice was provided either directly to the individual or through a public notice? What procedures are in place to ensure that information is used only for the purpose articulated in the notice?
This question is related to privacy control TR-1, Privacy Notice, AR-2, Privacy Impact and Risk Assessment, and UL-1, Internal Use.
Follow the format below:

Privacy Risk: There is a risk that individuals will not know how their information is being shared and used internal to the Department of Veterans Affairs within ServiceNow Support.

Mitigation: The VA ensures that it provides individuals with a notice of information collection and notice of the system's existence through the applicable SORN.

- 17VA26 / 78 FR 71727 - Loan Guarantee Fee Personnel and Program Participant Records-VA
- 27VA047 / 77 FR 39346 - Personnel & Acct Integrated Data system
- 55VA26 - Loan Guaranty Home, Condominium and Manufactured Home Loan Applicants Records
- 168VA005 / 86 FR 6975 - Health Information Exchange
- 24VA10A7 / 85 FR 62406 - Patient Medical Records-
- VA146VA005Q3 / 73 FR 16093 – Department of Veterans Affairs Identity Management System (VAIDMS)

The VA provides the public with two forms of notice that the system exists, including the Privacy Impact Assessment (PIA) and the SORN. This PIA is a form of notice.

Section 7. Access, Redress, and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about him or her.

7.1 What are the procedures that allow individuals to gain access to their information?

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 http://www.foia.va.gov/ to obtain information about FOIA points of contact and information about agency FOIA processes.***

In accordance to VA Directive 6300, Records and Information Management (https://vaww.va.gov/vapubs/viewPublication.asp),6300.4, Procedures for Processing Requests for Records Subject to the Privacy Act (https://vaww.va.gov/vapubs/viewPublication.asp?Pub_ID=701&FType=2), and VHA Directive 1605, VHA Privacy Program, (https://vaww.va.gov/vhapublications/ViewPublication.asp?pub_ID=5456) an individual's submitting information requests may be used as the written request requirement. All requests to review must be received by direct mail, fax, in person, or by mail referral from another agency or VA office. All requests for access must be delivered to and reviewed by the System Manager for the concerned system of records, Privacy Officer, or their designee. Each request must be date stamped and reviewed to determine whether the

request for access should be granted. The system manager then releases approved information to the FOIA Office, and the FOIA Office is responsible for assessing if all the information may be released or if redacting or segregating is required.

The following SORN explain the Record Access Record Access Procedures.

- 17VA26 / 78 FR 71727 - Loan Guarantee Fee Personnel and Program Participant Records-VA
- 27VA047 / 77 FR 39346 - Personnel & Acct Integrated Data system
- 55VA26 - Loan Guaranty Home, Condominium and Manufactured Home Loan Applicants Records
- 168VA005 / 86 FR 6975 - Health Information Exchange
- 24VA10A7 / 85 FR 62406 - Patient Medical Records-
- VA146VA005Q3 / 73 FR 16093 – Department of Veterans Affairs Identity Management System (VAIDMS)

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)?

This system is not exempt from the access provisions of the Privacy Act. Individuals seeking information on the existence and content of records in pertaining to them should refer to the source system SORN.

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?

This system is not exempt from the access provisions of the Privacy Act. Individuals seeking information on the existence and content of records in pertaining to them should refer to the source system SORN.

- 17VA26 / 78 FR 71727 - Loan Guarantee Fee Personnel and Program Participant Records-VA
- 27VA047 / 77 FR 39346 - Personnel & Acct Integrated Data system
- 55VA26 - Loan Guaranty Home, Condominium and Manufactured Home Loan Applicants Records
- 168VA005 / 86 FR 6975 - Health Information Exchange
- 24VA10A7 / 85 FR 62406 - Patient Medical Records-
- VA146VA005Q3 / 73 FR 16093 – Department of Veterans Affairs Identity Management System (VAIDMS)

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.

All data within the Service Now Support system is collected through ServiceNow (GCC-E). Individuals seeking to contest or amend records in this system should contact the source system manager in writing as indicated in the applicable SORN. A request to contest or amend records must state clearly and concisely what record is being contested, the reasons for contesting it, and the proposed amendment to the record.

- 17VA26 / 78 FR 71727 - Loan Guarantee Fee Personnel and Program Participant Records-VA
- 27VA047 / 77 FR 39346 - Personnel & Acct Integrated Data system
- 55VA26 - Loan Guaranty Home, Condominium and Manufactured Home Loan Applicants Records
- 168VA005 / 86 FR 6975 - Health Information Exchange
- 24VA10A7 / 85 FR 62406 - Patient Medical Records-
- VA146VA005Q3 / 73 FR 16093 – Department of Veterans Affairs Identity Management System (VAIDMS)

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 SORN and the PIA are ways that individuals are notified. Individuals seeking to contest or amend records in the source system should contact the system manager in writing as indicated in the applicable SORN. A request to contest or amend records must state clearly and concisely what record is being contested, the reasons for contesting it, and the proposed amendment to the record.

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.

ServiceNow Support does not provide a formal redress process. All data within the Service Now

Support system is collected through ServiceNow (GCC-E) and GCC-E obtains data via various source systems. Formal redress is provided within the various source system and information on this process is found in the SORN.

- 17VA26 / 78 FR 71727 - Loan Guarantee Fee Personnel and Program Participant Records-VA
- 27VA047 / 77 FR 39346 - Personnel & Acct Integrated Data system
- 55VA26 - Loan Guaranty Home, Condominium and Manufactured Home Loan Applicants Records
- 168VA005 / 86 FR 6975 - Health Information Exchange
- 24VA10A7 / 85 FR 62406 - Patient Medical Records-
- VA146VA005Q3 / 73 FR 16093 – Department of Veterans Affairs Identity Management System (VAIDMS)

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 System ISSO to complete all Privacy Risk questions inside the document this section).*

Consider the following FIPPs below to assist in providing a response:
Principle of Individual Participation: Is the individual provided with the ability to find out whether a project maintains a record relating to him?

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

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

Follow the format below:

Privacy Risk: There is a risk that data contained within the various source systems is incorrect and individuals could be unaware of access, redress, and correction procedures.

Mitigation: No personal data is collected directly from individuals. Information is gathered from various source systems. The PIA and the applicable SORN from the source system are available to be referenced as needed. These publicly available documents would cover the information access procedures.

Section 8. Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

8.1 What procedures are in place to determine which users may access the system, and are they documented?

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?

ServiceNow Support is only accessible by other systems connecting to collect data. ServiceNow Support team requiring access will comply with VA Platform One (VAPO) access control policies and procedures, including submitting an Elevated Privilege Account request.

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?

A VA Manager or Supervisor will approve all users who will access ServiceNow Support. The Information System Owner (ISO) will evaluate all external agency requests and sharing of all data.

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.

A VA manager or supervisor will approve all users who will access ServiceNow Support. All users within the VA Identity and Access Management (IAM), Microsoft Entra and Lightweight Directory Access Protocol (LDAP) are not provisioned for access to ServiceNow Support as a standard user account (SUA) with general access. If an account with higher access is needed, a request will need to be submitted by the user's VA manager or supervisor for approval.

Below is the list of general roles to access VA ServiceNow:

1. Standard User Accounts (SUA) – issued for routine non-privileged access. These accounts will be enforced for two-factor (PIV Card) using Single Sign On for users on a VA network. SUAs will be mailbox enabled.
2. Administrator/Privileged Accounts – issued to accomplish administrative tasks requiring privileged access on VA information systems. These accounts are separate from the SUA and are Non-Mailbox Enabled Accounts (NMEA).
3. Service Accounts – used by a service, program, application, or other process requiring authentication. Service accounts must have an identified Account Custodian. The custodian will be configured as the account "Manager" and will be identified in the description attribute of the account. These accounts are maintained by the VA IO ServiceNow Platform Owners group.

8.2 Will VA contractors have access to the system and the PII? If yes, what involvement will contractors have with the design and maintenance of the system? Has a contractor confidentiality agreement, Business Associate Agreement (BAA), or a Non-Disclosure Agreement (NDA) been developed for contractors who work on the system?

If so, how frequently are contracts reviewed and by whom? Describe the necessity of the access provided to contractors to the system and whether clearance is required. If Privacy Roles and Responsibilities have been established to restrict certain users to different access levels, please describe the roles and associated access levels. Explain the need for VA contractors to have access to the PII. This question is related to privacy control AR-3, Privacy Requirements for Contractors, and Service Providers.

Yes. There are contract system administration personnel who operate and maintain the cloud infrastructure but who are not users of ServiceNow Support. Contractors sign an NDA for their employment. The contractors who provide support to the system are required to complete annual VA Privacy and Information Security and Rules of Behavior training via the VA TMS. Contractors will have authorized access to this system for development purposes. All contractors are cleared using the VA background investigation process and must obtain a Minimum Background Investigation (MBI). ServiceNow components employ the same security mechanisms.

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.

All individuals must complete all required VA Talent Management System (TMS) training for Privacy and HIPPA before being onboarded to the contract. The training records are retained for 7 years. This documentation and monitoring are performed using the VA TMS.

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

8.4a If yes, provide:

1. *The Security Plan Status:* Approved
2. *The System Security Plan Status Date:* 17-Mar-2023
3. *The Authorization Status:* Authorization to Operate (ATO)
4. *The Authorization Date:* 15-Jun-2023
5. *The Authorization Termination Date:* 14-Jun-2025
6. *The Risk Review Completion Date:* 14-Jun-2023
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* High

Please note that all systems containing SPI are categorized at a minimum level of "moderate" under Federal Information Processing Standards Publication 199.
8.4b If No or In Process, provide your ***Initial Operating Capability (IOC) date.***

Not applicable.

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.

Note: For systems utilizing the VA Enterprise Cloud (VAEC), no further responses are required after 9.1*. (Refer to question 3.3.1 of the PTA)*

Software as a Service (SaaS)" and "VAEC Microsoft Azure."

9.2 Does the contract with the Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII? (Provide contract number and supporting information about PII/PHI from the contract). (*Refer to question 3.3.2 of the PTA) This question is related to privacy control AR-3, Privacy Requirements for Contractors, and Service Providers.*

Yes, the VA owns all records and data within ServiceNow Support.

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.

Yes, the VA owns all records and data within ServiceNow Support.

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.

Yes, the VA owns all records and data within the ServiceNow Support.

9.5 If the system is utilizing Robotics Process Automation (RPA), please describe the role of the bots.

Robotic Process Automation is the use of software scripts to perform tasks as an automated process that executes in parallel with or in place of human input. For example, will the automation move or touch PII/PHI information. RPA may also be referred to as "Bots" or Artificial Intelligence (AI).

No, VA ServiceNow Support does not use Robotics Process Automation.

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: 2024.06.04 15:36:17 -05'00'

Privacy Officer, Gina Siefert

YENTL BROOKS Digitally signed by YENTL BROOKS
Date: 2024.06.04 15:10:02 -05'00'

Information Systems Security Officer,- Yentl Brooks

PRASHANTHI KUCHIKULLA Digitally signed by PRASHANTHI KUCHIKULLA
Date: 2024.06.04 18:52:44 -04'00'

Information Systems Owner, Prashanthi Kuchikulla

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).

Access to ServiceNow Support is contingent on implied consent within the VA National Rules of Behavior. https://www.va.gov/files/2021-12/Rules_of_behavior.pdf

HELPFUL LINKS:

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 Notice of Privacy Practices
VHA Handbook 1605.04: Notice of Privacy Practices